Cajun™
P550R®/P880/P882
Switch User Guide
Version 5.0

March 2001

Cajun P550R/P880/P882 Switch User Guide - Version 5.0

© Copyright Avaya Inc., 2001 ALL RIGHTS RESERVED

Produced in USA, March, 2001

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this document. Lucent disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

P550R is a registered trademark of Avaya Inc.

Avaya, Cajun, CajunDocs, OpenTrunk, CajunView, QIP, and RealNet are trademarks of Avaya Inc.

Microsoft, Windows, Windows NT, Windows 95, Windows 98, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

Sybase is a registered trademark of Sybase, Inc.

Novell, NDS, Netware, and Novell Directory Services are registered trademarks of Novell, Inc.

Solaris is a trademark of Sun Microsystems, Inc.

Intel and Pentium are registered trademarks of Intel Corporation.

ALL OTHER TRADEMARKS MENTIONED IN THIS DOCUMENT ARE PROPERTY OF THEIR RESPECTIVE OWNERS.

Table of Contents

Overview of the Contents 27
Technical Support 30
Avaya Technologies Products and Services 30
Conventions 31
    Using Notes, Cautions, and Warnings 33
Related Documentation 33
    Online Documentation 33
    Online Help 34
    Installing Online Documentation and Help Files 34
        Installing the HTTP Documentation Server 35
        Starting the HTTP Web Server 35
        Entering the Server Location on the Switch 35
        Adding Document Files to an Existing Server 36
        Downloading an Updated CajunDocs CD from the Internet 37
    Documentation 37
    Terminology 38
Documentation Feedback 38

Chapter 1 — Introduction to the Cajun P550R/P880/P882 Switch 1-1

Overview 1-1
Switch Description 1-1
Hardware Components 1-2
    Chassis 1-2
        50-Series Mode 1-2
        80-Series Mode 1-3
    P550R Chassis 1-3
        Slots 1-3
        Ports 1-3
        Fan Tray 1-4
        Power Supplies 1-4
        Switch Fabric 1-4
    P880/P882 Chassis 1-6
        Slots 1-6
        Ports 1-6
        Fan Tray 1-7
        Power Supplies 1-7
        Switch Fabric 1-7
    50-Series Modules 1-8
        Layer 2 Supervisor Module 1-8
        Layer 3 Supervisor Module 1-9

Redundant Supervisor 1-11
Media Modules 1-12
Layer 2 and Layer 3 Fast Ethernet Modules 1-13
Layer 2 and Layer 3 Gigabit-Speed Modules 1-13
ATM Uplink Module 1-13
80-Series Modules 1-14
Software Features 1-15
Virtual Bridging Functions 1-16
Flood Pruning Using VLANs 1-16
Hunt Groups 1-17
OpenTrunk Technology 1-17
Domain Naming System (DNS) Client Support 1-18
Remote Authentication Dial-In User Service (RADIUS) Client Support 1-19
OSPF Passive-Interface Support 1-19
Load MIB 1-20
Spanning Tree Modes 1-20
Spanning Tree Protocol Bridge Options 1-21
Global Disable 1-24
Extensive Fault Tolerance 1-25
Buffer and Queue Management 1-25
Routing Overview 1-26
Compatibility with the Layer 2 Switch 1-26
Routing with Layer 2 and Layer 3 Modules 1-27

Chapter 2 — Initialize and Setup of the P550R/P880/P882 Switch 2-1

Overview 2-1
Setting Up Your Laptop or PC Monitor 2-2
Configuring the Supervisor Module Using the CLI 2-2
Configuring the Switch Using the Web Agent 2-6
Opening the Web Agent 2-7
Moving through the Web Agent 2-9
Setting Up User Accounts 2-10
Setting Up User Accounts Using the Web Agent 2-10
Setting Up User Accounts Using the CLI 2-12
Setting Up SNMP Communities 2-12
Setting Up SNMP Communities Using the Web Agent 2-12
Setting Up SNMP Communities Using the CLI 2-14
Changing the Console Serial Port Settings 2-15
Configuring the Serial Console Port as a TTY Console 2-15
Configuring the Serial Console Port as a TTY Console Using the Web Agent 2-15
Configuring the Serial Console Port as a TTY Console Using the CLI 2-17
Configuring the Serial Console Port as a PPP Console 2-17
Connecting a Modem 2-18
Configuring the Serial Console Port as a PPP Console from the Web Agent 2-19

Configuring the Serial Console Port as a PPP Console Using the CLI 2-21
Regaining Configuration Access to the PPP Serial Port Console 2-22
Configuring Dial-Up Networking 2-22
Using Dial-Up Networking with a PPP Serial Port Console 2-24
Managing Configuration Files 2-25
Viewing Your Running Configuration 2-25
Viewing Your Startup Configuration 2-25
Viewing Your Script Execution Log File 2-26
Viewing Your Script Execution Log File Using the Web Agent 2-26
Viewing Your Script Execution Log File Using the CLI 2-26
Copying Configuration Files 2-26
Copying the Running Configuration to the Startup Configuration Using the Web Agent 2-26
Copying the Running Configuration to the Startup Configuration Using the CLI 2-27
Copying Files 2-27
Copy Files Using the Web Agent 2-27
Copying Files Using the CLI 2-30
Viewing the Status of a TFTP Transfer 2-31
Viewing the Status of a TFTP Transfer Using the Web Agent 2-31
Viewing the Status of a TFTP Transfer Using the CLI 2-31

Chapter 3 — Configuring System Information 3-1

Overview 3-1
Managing System Information 3-1
Entering General System Information 3-2
Entering General System Information Using the Web Agent 3-2
Enabling the Simple Network Time Protocol (SNTP) 3-3
Setting Summer Time Hours 3-4
Setting Recurring Summer Time Hours 3-5
Setting One-Time Summer Time Hours 3-9
Setting the System Clock 3-11
Setting the System Clock Using the Web Agent 3-11
Setting the System Clock Using the Web Agent 3-12
Setting the Temperature System 3-13
Setting the Temperature System Using the Web Agent 3-13
Setting the Temperature System Using the CLI 3-14
Displaying the Power System Statistics 3-14
Displaying the Power System Statistics Using the Web Agent 3-14
Displaying the Power System Statistics Using the CLI 3-15
Displaying Cooling System Statistics 3-16

Displaying the Cooling System Statistics Using the Web Agent 3-16
Displaying the Cooling System Statistics Using the CLI 3-16
Performing a Reset 3-17
Performing a Reset Using the Web Agent 3-17
Performing a Reset Using the CLI 3-17

Chapter 4 — Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping 4-1

Overview 4-1
VLAN Operation 4-1
Ingress Rules 4-2
Forwarding Rules 4-2
Egress Rules 4-3
Port-Based VLANs 4-3
Creating and Implementing VLANs 4-3
VLAN Considerations 4-3
Creating a VLAN 4-4
Configuring VLAN Parameters 4-7
Creating 3Com Mapping Tables 4-8
Creating 3Com Mapping Tables Using the Web Agent 4-9
Creating 3Com Mapping Tables Using the CLI 4-10
Assigning Ports to VLANs 4-10
Using Spanning Tree Setup and Monitoring 4-10
Managing Spanning Tree 4-10
Managing Spanning Tree Using the Web Agent 4-10
Managing Spanning Trees Using the CLI 4-13
Configuring Spanning Tree Bridge Ports 4-13
Configuring Spanning Tree Bridge Ports Using the Web Agent 4-13
Configuring Spanning Tree Bridge Ports Using the CLI 4-16
Disabling Spanning Tree Mode for the Port 4-17
Disabling Spanning Tree Mode for the Port Using the Web Agent 4-17
Disabling Spanning Tree Mode on a Port Using the CLI 4-19
Using Hunt Groups to Aggregate Bandwidth between Switches 4-20
Features 4-20
How Hunt Groups Load Share 4-21
Hunt Group Considerations 4-25
Creating Hunt Groups 4-25
Creating Hunt Groups Using the Web Agent 4-25
Creating Hunt Groups Using the CLI 4-28
Viewing Hunt Group Members 4-29
Viewing Hunt Group Members Using the Web Agent 4-29
Viewing Hunt Group Members Using the CLI 4-29
Adding Ports to a Hunt Group 4-30
Adding Ports to a Hunt Group Using the Web Agent 4-30
Adding Ports to a Hunt Group Using the CLI 4-32

Configuring VLAN Trunk Protocol (VTP) Snooping 4-32
Configuring VTP Snooping Using the Web Agent 4-33
Configuring VTP Snooping Using the CLI 4-36

Chapter 5 — Configuring Port Parameters 5-1

Overview 5-1
Configuring Port Parameters 5-1
Physical Port Features 5-2
Auto-negotiation 5-2
Flow Control 5-3
Switch Port Features 5-5
Creating Virtual LANs (VLANs) 5-5
Manual VLAN Creation 5-5
Automatic VLAN Creation 5-6
VLAN Operational Rules 5-7
Ingress Rules 5-7
Forwarding Rules 5-8
Egress Rules 5-8
Relationship Between Different Switch Port Parameters 5-9
Assigning VLANs to a Port and Associated Issues 5-12
Configuring Physical Port Parameters on Gigabit Ports 5-14
Configuring Physical Port Parameters on Gigabit Ports Using the Web Agent 5-14
Configuring Physical Port Parameters on Gigabit Ports Using the CLI 5-18
Configuring Physical Port Parameters on Fast Ethernet Ports 5-19
Configuring Physical Port Parameters using the Web Agent 5-19
Configuring Physical Port Parameters on Fast Ethernet Ports Using the CLI 5-25
Using the All Ports Configuration Window 5-26
Viewing Switch Port Parameters 5-28
Viewing Switch Port Parameters Using the Web Agent 5-28
Viewing Switch Port Parameters Using the CLI 5-29
Configuring Switch Port Parameters 5-30
Configuring Switch Port Parameters Using the Web Agent 5-30
Configuring Switch Ports Using the CLI 5-32
Configuring Port VLAN Parameters 5-33
Configuring Port VLAN Parameters Using the Web Agent 5-33
Configuring Port VLAN Parameters Using the CLI 5-34
Configuring Non-VLAN Switch Port Parameters 5-35
Configuring Non-VLAN Switch Port Parameters Using the Web Agent 5-35
Configuring Non-VLAN Switch Port Parameters Using the CLI 5-37

Configuring Fast Start Mode 5-37
Configuring Fast Start Mode Using the Web Agent 5-38
Configuring Fast Start Mode Using the CLI 5-40
Using the All Module Ports Configuration Window 5-40

Chapter 6 — Managing the Address Forwarding Table 6-1

Overview 6-1
Configuring the Address Forwarding Table (AFT) 6-1
Configuring the Age Timer and Super Age Timer 6-2
Configuring the Age Timer and Super Age Timer Using the Web Agent 6-2
Configuring the Age Timer and Super Age Timer Using the CLI 6-3
Controlling Reconfiguration of AFT Sizes 6-3
Controlling Reconfiguration of AFT Sizes Using the Web Agent 6-4
Controlling Reconfiguration of AFT Sizes Using the CLI 6-8
Searching the Switch AFT 6-8
Searching the Switch AFT Using the Web Agent 6-8
Searching the Switch AFT Using the CLI 6-12
Adding Entries to the AFT Manually 6-13
Adding Entries to the AFT Manually Using the Web Agent 6-13
Adding Entries to the AFT Manually Using the CLI 6-14

Chapter 7 — Configuring Redundancy Options 7-1

Overview 7-1
Configuring Redundant Hardware 7-2
Installing Redundant Hardware 7-4
Enabling Redundant Hardware 7-5
Enabling Redundant Hardware Using the Web Agent 7-5
Replacing the Primary Controller 7-6
Replacing an Element 7-7
Enabling a Replaced Element Using the Web Agent 7-8
Enabling a Replaced Element Using the CLI 7-8
Configuring a Redundant CPU 7-9
Configuring a Redundant CPU Using the Web Agent 7-9
Configuring a Redundant CPU Using the CLI 7-9
Synchronizing the Primary and Redundant CPUs 7-10
Synchronizing the Primary and Redundant CPUs Using the Web Agent 7-10
Synchronizing the Primary and Redundant CPUs Using the CLI 7-11

Chapter 8 — Configuring DNS and RADIUS Clients 8-1

Overview 8-1
Configuring a Domain Name System Client 8-1

Configuring a DNS Client Using the Web Agent 8-2
Configuring a DNS Client Using the CLI 8-3
Configuring a Remote Authentication Dial-In User Service (RADIUS) Client 8-3
Configuring a RADIUS Client Using the Web Agent 8-4
Configuring a RADIUS Client Using the CLI 8-5

Chapter 9 — Configuring IP Routing 9-1

Overview 9-1
Configuring Internet Protocol (IP) Global Routing 9-1
Creating an IP Interface 9-2
Creating an IP Interface Using the Web Agent 9-2
Creating an IP Interface Using the CLI 9-8
Enabling IP Routing 9-8
Enabling IP Routing Using the Web Agent 9-8
Creating an IP Interface Using the CLI 9-10
Configuring IP Routing on the Switch 9-10
Hardware Requirements for Routing 9-11
Minimum IP Routing Configuration Requirements 9-11
Routing Configuration Quickstart 9-11
Assigning IP Interfaces to the VLAN 9-12
IP Multinetting 9-12
Creating a Multinet Interface 9-13
Configuring Access Lists 9-14
Creating Standard Access Rules 9-14
Creating Extended Access Rules 9-16
Activating Access Lists 9-22
Activating Access Lists Using the Web Agent 9-22
Activating Access Lists Using the CLI 9-23
Creating IP Static Routes 9-23
Creating IP Static Routes Using the Web Agent 9-23
Creating IP Static Routes Using the CLI 9-24
Creating IP Static ARP Entries 9-24
Creating IP Static ARP Entries Using the Web Agent 9-24
Creating IP Static ARP Entries Using the CLI 9-26
Creating a BOOTP/DHCP Server Entry 9-26
Creating a BOOTP/DHCP Server Entry Using the Web Agent 9-26
Creating a BOOTP/DHCP Server Entry Using the CLI 9-27
IP Multicast 9-27
Configuring IGMP 9-28
Globally Enabling IGMP Using the Web Agent 9-29
Globally Enabling IGMP Using the CLI 9-30
Modifying IGMP Interfaces Using the Web Agent 9-30
Modifying IGMP Interfaces Using the CLI 9-32
Configuring and Modifying Distance Vector Multicast Routing Protocol (DVMRP) 9-33
Configuring the DVMRP Global Configuration Using the

Web Agent 9-33
Configuring the DVMRP Global Configuration Using the CLI 9-36
Modifying a DVMRP Interface 9-36
Modifying the DVMRP Interface Using the Web Agent 9-36
Modifying the DVMRP Global Configuration Using the CLI 9-38
Monitoring Switch Performance Using IP Statistics 9-38
Displaying Global IP Routing Statistics 9-38
Displaying Global IP Routing Statistics Using the Web Agent 9-38
Displaying Global IP Routing Statistics Using the CLI 9-44
Searching the IP Routing Table 9-44
Displaying the IP Routing Table Statistics 9-46
Searching the IP ARP Cache 9-47
IP Multicast Statistics 9-48
Displaying IGMP Global Statistics Using the Web Agent 9-49
Displaying IGMP Global Statistics Using the CLI 9-50
Displaying IGMP Interface Statistics 9-50
Displaying IGMP Interface Statistics Using the Web Agent 9-50
Displaying IGMP Interface Statistics Using the CLI 9-52
Displaying the Multicast Group Table 9-52
Displaying the IGMP Local Multicast Forwarding Cache 9-53
Displaying DVMRP Global Statistics 9-54
Displaying DVMRP Interface Statistics 9-56
Displaying DVMRP Neighbor Router(s) 9-58
Displaying DVMRP Routing Table Statistics 9-59
Displaying the DVMRP Route Table 9-60
Displaying the DVMRP Upstream Routers 9-61
Displaying the DVMRP Designated Forwarder(s) Table 9-62
Displaying the DVMRP Downstream Dependent Router(s) 9-62
Displaying the DVMRP Multicast Forwarding Cache 9-63
Configuring Virtual Redundant Router Protocol (VRRP) 9-67
Globally Enabling VRRP 9-67
Globally Enabling VRRP Using the Web Agent 9-67
Globally Enabling VRRP Using the CLI 9-68
Enabling VRRP on an Interface 9-69
Enabling VRRP on an Interfere Using the Web Agent 9-69
Enabling VRRP on an Interface Using the Web Agent 9-70
Creating a VRRP Virtual Router 9-70
Creating a VRRP Virtual Router Router Using the Web Agent 9-70
Creating a VRRP Virtual Router Router Using the CLI 9-72
Displaying VRRP Statistics 9-72
Displaying VRRP Router Statistics using the Web Agent 9-72
Displaying VRRP Router Statistics using the CLI 9-73
Configuring ICMP Router Discovery Protocol (IRDP) 9-74

Enabling IRDP on an Interface 9-74
Enabling IRDP on an Interface Using the Web Agent 9-74
Enabling IRDP on an Interface Using the CLI 9-77
Configuring Lightweight Directory Access Protocol (LDAP) 9-77
Configuring LDAP Settings 9-78
Configuring LDAP Settings from the Web Agent 9-78
Configuring LDAP Settings from the CLI 9-79
Viewing LDAP Statistics Using the Web Agent 9-80
Viewing LDAP Statistics Using the CLI 9-81
Configuring a Static Route for the PPP Console 9-81
Configuring the IP Interface for the PPP Console 9-83
Configuring the IP Interface for the PPP Console Using the Web Agent 9-83
Configuring the IP Interface for the PPP Console Using the CLI 9-85

Chapter 10 — Configuring the Routing Information Protocol (RIP) 10-1

Overview 10-1
Configuring RIP on the Switch 10-1
Configuring RIP on the Switch Using the Web Agent 10-1
Configuring RIP on the Switch Using the CLI 10-3
Modifying RIP Interfaces 10-3
Modifying RIP Interfaces Using the Web Agent 10-3
Modifying RIP Interfaces Using the CLI 10-5
Creating Trusted RIP Neighbors 10-6
Creating Trusted RIP Neighbors Using the Web Agent 10-6
Creating Trusted RIP Neighbors Using the CLI 10-7
Viewing RIP Statistics 10-7
Viewing RIP Statistics Using the Web Agent 10-7
Viewing RIP Statistics Using the CLI 10-8

Chapter 11 — Configuring the OSPF Routing Protocol 11-1

Overview 11-1
Configuring Open Shortest Path First (OSPF) 11-1
Configuring the OSPF Global Configuration 11-2
Configuring OSPF Globally Using the Web Agent 11-2
Configuring OSPF Globally Using the CLI 11-3
Creating OSPF Areas 11-4
Creating OSPF Areas Using the Web Agent 11-4
Creating OSPF Areas Using the CLI 11-5
Deleting OSPF Areas 11-6
Deleting an OSPF Area Using the Web Agent 11-6
Deleting an OSPF Area Using the CLI 11-6
Modifying OSPF Areas 11-6
Modifying an OSPF Area Using the Web Agent 11-6
Modifying an OSPF Area Using the CLI 11-6
Modifying OSPF Interfaces 11-7
Modifying OSPF Interfaces Using the Web Agent 11-7

Modifying OSPF Interfaces Using the CLI 11-9
Creating OSPF Virtual Links 11-9
Creating OSPF Virtual Links Using the Web Agent 11-9
Creating OSPF Virtual Links Using the CLI 11-11
Deleting OSPF Virtual Links 11-12
Deleting OSPF Virtual Links Using the Web Agent 11-12
Deleting OSPF Virtual Links Using the CLI 11-12
Modifying OSPF Virtual Links 11-12
Modifying OSPF Virtual Links Using the Web Agent 11-12
Modifying OSPF Virtual Links Using the CLI 11-13
Creating OSPF Summaries 11-13
Creating OSPF Summaries Using the Web Agent 11-13
Creating OSPF Summaries Using the CLI 11-14
Deleting OSPF Summaries 11-15
Deleting OSPF Summaries Using the Web Agent 11-15
Deleting OSPF Summaries Using the CLI 11-15
Modifying OSPF Summaries 11-15
Modifying OSPF Summaries Using the Web Agent 11-15
Modifying OSPF Summaries Using the CLI 11-16
Monitoring Switch Performance Using OSPF Statistics 11-16
Displaying OSPF Statistics 11-16
Displaying OSPF Statistics Using the Web Agent 11-16
Displaying OSPF Statistics Using the CLI 11-18
Displaying OSPF Links 11-18
Displaying OSPF Links Using the Web Agent 11-19
Displaying OSPF Links Using the CLI 11-19
Displaying OSPF Neighbors 11-20
Displaying OSPF Neighbors Using the Web Agent 11-20
Displaying OSPF Neighbors Using the CLI 11-22
Searching the OSPF Link State Database 11-22
Searching the OSPF Link State Database Using the Web Agent 11-23
Searching the OSPF Link State Database Using the CLI 11-28

Chapter 12 — Configuring IPX Routing 12-1

Overview 12-1
Internetwork Packet Exchange (IPX) Protocol Overview 12-1
IPX Datagram Structure 12-2
Configuring the Cajun Switch as an IPX Router 12-4
Hardware Requirements 12-4
Configuring IPX Routing Globally 12-4
Configuring IPX Routing Globally Using the Web Agent 12-4
Configuring IPX Routing Globally Using the CLI 12-5
Configuring IPX Interfaces 12-6
Configuring an IPX Interface Using the Web Agent 12-6
Configuring an IPX Interface Using the CLI 12-9
Creating IPX Static Routes 12-9
Creating IPX Static Routes Using the Web Agent 12-9

Creating IPX Static Routes Using the CLI 12-11
Deleting IPX Static Routes 12-11
Deleting IPX Static Routes Using the Web Agent 12-11
Deleting IPX Static Routes Using the CLI 12-11
Modifying IPX Static Routes 12-12
Modifying IPX Static Routes Using the Web Agent 12-12
Modifying IPX Static Routes Using the CLI 12-12
Creating IPX Static Services 12-13
Creating IPX Static Services Using the Web Agent 12-13
Creating IPX Static Services Using the CLI 12-14
Deleting IPX Static Service 12-15
Deleting IPX Static Service Using the Web Agent 12-15
Deleting IPX Static Service Using the CLI 12-15
Modifying IPX Static Service 12-15
Modifying IPX Static Service Using the Web Agent 12-15
Modifying IPX Static Service Using the CLI 12-16
Monitoring Your Switch Using IPX 12-16
Examine IPX Global Statistics 12-16
Examine IPX Global Statistic Using the Web Agent 12-16
Examine IPX Global Statistic Using the CLI 12-18
Search the IPX Route Table 12-19
Examine the IPX Route Table 12-20
Examine IPX Route Table Statistics 12-21
Search the IPX Service Table 12-21
Examine the IPX Service Table 12-23
Examine IPX Service Table Statistics 12-24

Chapter 13 — Configuring IPX RIP Protocol 13-1

Overview 13-1
Configuring Internetwork Packet Exchange (IPX) Routing Interface Protocol (RIP) Interfaces 13-1
Configuring IPX RIP Interfaces Using the Web Agent 13-1
Configuring IPX RIP Interfaces Using the CLI 13-3
Creating and Modifying IPX RIP Filters 13-3
Creating and Modifying IPX RIP Filters Using the Web Agent 13-3
Creating and Modifying IPX RIP Filters Using the CLI 13-7

Chapter 14 — Configuring IPX SAP Protocol 14-1

Overview 14-1
Configuring Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) Interfaces 14-1
Configuring IPX SAP Interfaces Using the Web Agent 14-1
Configuring IPX SAP Interfaces Using the CLI 14-3
Creating IPX SAP Filters 14-4
Creating IPX SAP Name Filters 14-4
Creating IPX SAP Name Filters Using the Web Agent 14-4
Creating IPX SAP Name Filters Using the CLI 14-7

Creating IPX SAP Network Filters 14-8
Creating IPX SAP Network Filters Using the Web Agent 14-8
Creating IPX SAP Network Filters Using the CLI 14-12
Interpreting IPX SAP Interface Statistics 14-12
Interpreting IPX SAP Interface Statistics Using the Web Agent 14-12
Interpreting IPX SAP Interface Statistics Using the CLI 14-13

Chapter 15 — Configuring AppleTalk Routing 15-1

Overview 15-1
AppleTalk Routing Overview 15-1
Configuring AppleTalk Routing 15-2
Enabling AppleTalk Global Routing 15-3
Creating an AppleTalk Routing Interface 15-3
Creating an AppleTalk Routing Interface Using the Web Agent 15-3
Creating an AppleTalk Routing Interface Using the CLI 15-7
Editing AppleTalk Interfaces 15-7
Editing AppleTalk Interfaces Using the Web Agent 15-7
Editing AppleTalk Interfaces Using the CLI 15-9
Deleting an AppleTalk Interface 15-9
Deleting an AppleTalk Interface Using the Web Agent 15-9
Deleting an AppleTalk Interface Using the CLI 15-9
Creating an AppleTalk Static Route 15-10
Creating an AppleTalk Static Route Using the Web Agent 15-10
Creating an AppleTalk Static Route Using the CLI 15-11
Editing AppleTalk Static Routes 15-12
Editing AppleTalk Static Routes Using the Web Agent 15-12
Editing AppleTalk Static Routes Using the CLI 15-12
Deleting an AppleTalk Static Route 15-13
Deleting an AppleTalk Static Route Using the Web Agent 15-13
Deleting an AppleTalk Static Route Using the CLI 15-13
Creating an AppleTalk Name-Binding Protocol (NBP) Filter 15-13
Creating a NBP Filter Using the Web Agent 15-14
Creating a NBP Filter Using the CLI 15-15
Editing an AppleTalk NBP Filter 15-16
Editing an AppleTalk NBP Filter Using the Web Agent 15-16
Editing an AppleTalk NBP Filter Using the CLI 15-16
Adding or Deleting Interfaces to an NBP Filter 15-17
Adding or Deleting Interfaces to an NBP Filter Using the Web Agent 15-17
Adding or Deleting Interfaces to NBP Filter Using the CLI 15-18
Creating an AppleTalk Zone Filter 15-18
Creating an AppleTalk Zone Filter Using the Web Agent 15-

18
Creating an AppleTalk Zone Filter Using the CLI 15-19
Editing an AppleTalk Zone Filter 15-20
Editing an AppleTalk Zone Filter Using the Web Agent 15-20
Editing an AppleTalk Zone Filter Using the CLI 15-20
Adding or Deleting Interfaces to a Zone Filter 15-21
Adding or Deleting Interfaces to a Zone Filter Using the Web Agent 15-21
Adding or Deleting Interfaces to a Zone Filter Using the CLI 15-22
Viewing AppleTalk Statistics 15-22
Viewing AppleTalk Global Statistics 15-23
Viewing AppleTalk Global Statistics Using the Web Agent 15-23
Viewing AppleTalk Global Statistics Using the CLI 15-25
Viewing the AppleTalk Interface Statistics Table 15-26
Viewing the AppleTalk Interface Statistics Table Using the Web Agent 15-26
Viewing the AppleTalk Interface Statistics Table Using the CLI 15-27
Viewing the AppleTalk Route Table 15-27
Viewing the AppleTalk Route Table Using the Web Agent 15-27
Viewing the AppleTalk Interface Statistics Table Using the CLI 15-29
Viewing AppleTalk Route Table Statistics 15-29
Viewing AppleTalk Route Table Statistics Using the Web Agent 15-29
Viewing AppleTalk Route Table Statistics Using the CLI 15-30
Viewing the AppleTalk ARP Cache Table 15-30
Viewing the AppleTalk ARP Cache Table Using the Web Agent 15-30
Viewing the AppleTalk ARP Cache Table Using the CLI 15-31
Viewing the AppleTalk Zone Table 15-32
Viewing the AppleTalk Zone Table Using the Web Agent 15-32
Viewing the AppleTalk Zone Table Using the CLI 15-32
Viewing AppleTalk Zone Table Statistics 15-33
Viewing AppleTalk Zone Table Statistics Using the Web Agent 15-33
Viewing AppleTalk Zone Table Statistics Using the CLI 15-33
Viewing the AppleTalk NBP Table 15-34
Viewing the AppleTalk NBP Table Using the Web Agent 15-34
Viewing the AppleTalk NBP Table Using the CLI 15-34

Chapter 16 — Managing Intelligent Multicasting 16-1

Overview 16-1
Introduction 16-1
- Layer 3 Dynamic Intelligent Multicasting 16-2
  - IGMP Snooping 16-3
  - LGMP Server 16-3
- Layer 2 Dynamic Intelligent Multicasting 16-3
  - LGMP Client 16-3
  - CGMP Snooping 16-3
  - Pruning Dynamic Sessions, Client Ports, and Router Ports 16-4

Configuring Intelligent Multicasting 16-4
- Configuring Global Intelligent Multicasting 16-5
  - Configuring Global Intelligent Multicasting Using the Web Agent 16-5
  - Configuring Global Intelligent Multicasting Using the CLI 16-7
- Displaying Router Ports 16-7
  - Displaying Router Ports Using the Web Agent 16-7
  - Displaying Router Ports Using the CLI 16-8
- Configuring Static Router Ports 16-8
  - Configuring Static Router Ports Using the Web Agent 16-8
  - Configuring Static Router Ports Using the CLI 16-9
- Searching for Intelligent Multicast Sessions 16-9
  - Searching for Intelligent Multicast Sessions Using the Web Agent 16-9
  - Searching for Intelligent Multicast Sessions Using the CLI 16-12
- Deleting an Intelligent Multicast Session 16-12
  - Deleting an Intelligent Multicast Session Using the Web Agent 16-12
  - Deleting a Multicast Session Using the CLI 16-12
- Deleting a Multicast Session Client Port 16-13
  - Deleting a Multicast Session Client Port Using the Web Agent 16-13
  - Deleting a Multicast Session Client Port Using the CLI 16-13
- Creating a Static Multicast Session 16-14
  - Creating a Static Multicast Session Using the Web Agent 16-14
  - Creating a Static Multicast Session Using the CLI 16-15
- Deleting Static Multicast Sessions 16-16
  - Deleting Static Multicast Sessions Using the Web Agent 16-16
  - Deleting Static Multicast Sessions Using the CLI 16-17
- Creating Static Client Ports 16-17
  - Creating Static Client Ports Using the Web Agent 16-17
  - Creating Static Client Ports Using the CLI 16-18
- Deleting Static Client Ports 16-18

Deleting Static Client Ports Using the Web Agent 16-18
Deleting Static Client Ports Using the CLI 16-18
Configuring Internet Group Management Protocol (IGMP) Snooping (Multilayer only) 16-18
Enabling IGMP Snooping 16-19
Enabling IGMP Snooping Using the Web Agent 16-19
Enabling IGMP Snooping Using the CLI 16-19
Configuring IGMP Snooping 16-20
Configuring IGMP Snooping Using the Web Agent 16-20
Configuring IGMP Snooping Using the CLI 16-21
Configuring the Lucent Group Management Protocol (LGMP) Server 16-21
Enabling the LGMP Server 16-21
Enabling the LGMP Server Using the Web Agent 16-22
Enabling the LGMP Server Using the CLI 16-23
Configuring the LGMP Server 16-23
Configuring the LGMP Server Using the Web Agent 16-23
Configuring the LGMP Server Using the CLI 16-26
Modifying the LGMP Server Display per VLAN 16-26
Modifying the LGMP Server Display per VLAN Using the Web Agent 16-26
Modifying the LGMP Server Display per VLAN Using the Web Agent 16-28
Configuring/Viewing an LGMP Client 16-29
Enabling/Viewing an LGMP Client Using the Web Agent 16-29
Enabling/Viewing an LGMP Client Using the CLI 16-31
Modifying LGMP Clients Per VLAN 16-31
Modifying LGMP Clients Per VLAN Using the Web Agent 16-31
Modifying LGMP Clients Per VLAN Using the CLI 16-33
Enabling/Viewing Cisco Group Management Protocol (CGMP) Snooping 16-33
Enabling/Viewing CGMP Snooping Using the Web Agent 16-33
Enabling/Viewing CGMP Snooping Using the CLI 16-35

Chapter 17 — Monitoring the Cajun Switch 17-1

Overview 17-1
Interpreting Front Panel LED Displays 17-1
Checking Temperature Status and Configuring Thresholds 17-2
Checking Temperature Status and Configuring Thresholds 17-2
Checking Temperature Status and Configuring Thresholds Using the Web Agent 17-3
Checking Temperature Status and Configuring Thresholds Using the CLI 17-4
Checking Active Alarms 17-5
Viewing the Active Alarm Table 17-5

Viewing the Active Alarm Table Using the Web Agent 17-5
Viewing the Active Alarm Table Using the CLI 17-6
Using the Event Subsystem 17-7
Configuring the Protocol Event Log 17-7
Configuring the Protocol Event Log Using the Web Agent 17-7
Configuring the Protocol Event Log Using the CLI 17-10
Viewing the Event and Shutdown Logs 17-10
Viewing the Event and Shutdown Logs Using the Web Agent 17-10
Viewing the Event and Shutdown Logs Using the CLI 17-12
Viewing Event Statistics 17-13
Viewing Event Statistics Using the Web Agent 17-13
Viewing Event Statistics Using the CLI 17-14
Setting Log Size 17-14
Setting Log Size Using the Web Agent 17-14
Setting Log Size Using the CLI 17-16
Configuring Event Notification 17-16
Configuring Event Notification Using the Web Agent 17-16
Configuring Event Notification Using the CLI 17-17

Chapter 18 — Monitoring and Configuring the Forwarding Cache 18-1

Overview 18-1
Configuring the Fowarding Cache 18-1
Configuring the Forwarding Cache Using the Web Agent 18-1
Configuring the Fowarding Cache Using the CLI 18-4
Monitoring the Forwarding Cache Statistics 18-5
Displaying Frame Fowarding Statistics 18-5
Displaying Frame Fowarding Statistics Using the Web Agent 18-5
Displaying Frame Fowarding Statistics Using the CLI 18-7
Searching the Routing Cache for an Entry 18-7
Searching the Routing Cache for an Entry Using the Web Agent 18-7
Searching the Routing Cache for an Entry Using the CLI 18-9
Displaying the Forwarding Cache 18-10
Displaying the Forwarding Cache Using the Web Agent 18-10
Displaying the Forwarding Cache Using the CLI 18-12

Chapter 19 — Analyzing Network Performance Using RMON and Ethernet Statistics 19-1

Overview 19-1
Viewing Network Statistics 19-1
Viewing Network Statistics Using the Web Agent 19-1

Viewing Network Statistics Using the CLI 19-7
Setting Up a Mirror Port 19-8
Setting Up a Mirror Port Using the Web Agent 19-8
Setting Up a Mirror Port Using the CLI 19-12

Chapter 20 — Tuning Your Switch Performance 20-1

Overview 20-1
How Queues Work 20-1
Managing Buffers and Queues 20-2
Managing Buffers and Queues Using the Web Agent 20-2
Managing Buffers and Queues Using the CLI 20-7

Appendix A — Downloading New Operational Code to the Switch A-1

Overview A-1
Upgrading from a Previous Version A-1
Saving the Previous Configuration A-2
Saving the Previous Configuration Using the Web Agent A-2
Saving the Previous Configuration Using the CLI A-3
Downloading a Software Image A-3
Downloading a Software Image Using the Web Agent A-3
Downloading a Software Image Using the CLI A-4
Selecting the Image for Reboot A-4
Selecting the Image for Reboot Using the Web Agent A-4
Selecting the Image for Reboot Using the CLI A-5
Resetting the Switch A-6
Resetting the Switch Using the Web Agent A-6
Resetting the Switch Using the CLI A-6

Appendix B — Boot Mode B-1

Accessing BOOT Mode B-1
Accessing BOOT Mode During Power Up B-1
Accessing BOOT Mode with Corrupted Operational Images B-2
Password Recovery B-3
Downloading New Operational Code B-3

Appendix C — Supported MIB Groups C-1

Management Information Bases (MIBs) Supported by Layer 2 and Multilayer Switches C-1
IPX Interface MIBs C-1
Private IPX Interface MIBs C-1
Prominet MIB C-1
IEEE 802.3 MAU Management C-2
IEEE 802.3 Statistics Group C-2
Bridge MIB C-2
SNMPv2 C-2
RMON C-2

MIBs Supported by the Multilayer Switch C-2
RIP Version 1.0 and 2.0 C-2
Standard MIB C-2
Private MIB C-2
OSPF Version 2.0 C-2
Standard MIB C-2
Private MIB C-3
VRRP C-3
Standard MIB C-3
Private MIB C-3
IGMP C-3
Standard MIB C-3
Private MIB C-3
IP Interface C-3
IP Version 4.0 and Services C-3
Standard MIB C-3
Private MIB C-3
IP Forwarding/Route Table C-4
Standard MIB C-4
Private MIB C-4
DVMRP C-4
Standard MIB C-4
Private MIB C-4
AppleTalk C-4
Standard MIB C-4
Private MIB C-4
IP Access List C-4
Policy Capability MIB for LDAP C-4
Load MIB Overview C-4
The genOperations group C-5
The genApplication Group C-5
MIB Specifications C-5

Appendix D — FCC Notice D-1

Table of Figures

Crossbar Architecture 1-5
Layer 3 Supervisor Conceptual Operation 1-10
Flooding Domain 1-17
Spanning Tree Models 1-21
Layer 2 and Layer 3 Routing in a Switch 1-28
Cajun P550R Switch Front View 2-2
Layer 2 and Layer 3 CLI Setup Command Session 2-5
Cajun Web Agent Welcome Window 2-7
Username and Password Required Window 2-8
System Information Window 2-8
Opening a Web Agent Folder 2-9
Operation Folder Contents 2-10
User Account Management Dialog Box 2-11
Add User Account Dialog Box. 2-11
SNMP Community Management Window 2-12
Create SNMP Community Dialog Box 2-13
Console Configuration Window 2-16
Console Port Configuration Window. 2-16
Typical Modem Connection to a Switch 2-18
Console Configuration Window 2-19
PPP Console Configuration Window. 2-20
System Reset Dialog Box 2-27
Configuration File Management Dialog Box 2-28
System Information Window 3-2
System Clock Dialog Box. 3-3
SNTP Client Configuration Dialog Box 3-4
System Clock Dialog Box 3-5
Summer Time Hours Dialog Box 3-6
System Clock Dialog Box 3-12
Temperature System Window 3-13
Power System Window 3-15
Cooling System Window 3-16
System Reset Page Window 3-17
VLAN Configuration Dialog Box 4-4
Create VLAN Dialog Box 4-5
VLAN Switch Ports Dialog Box 4-7
3Com Mapping Table Configuration Dialog Box (partial view) 4-9
Create 3Com Mapping Table Dialog Box 4-9

Spanning Tree Information Dialog Box 4-11
Spanning Tree Bridge Configuration Dialog Box 4-12
Spanning Tree Per Module Bridge Port Dialog Box 4-13
Spanning Tree Bridge Port Information Dialog Box 4-15
Module Information Dialog Box 4-18
Switch Ports Dialog Box 4-18
Switch Port Configuration Dialog Box 4-19
Load Sharing Example 4-22
Load Sharing PLEs 4-23
Load-Sharing Example 2 4-24
Module Information Dialog Box. 4-26
Physical Port Configuration Dialog Box. 4-27
Hunt Group Configuration Dialog Box. 4-28
Create Hunt Group Dialog Box. 4-28
Hunt Group Members Dialog Box. 4-29
Switch Ports Dialog Box 4-30
Switch Port Configuration Dialog Box. 4-31
Module Information Window 4-33
Switch Ports Window 4-33
Switch Port Configuration Window with VTP Options 4-34
VTP Snooping Configuration Window 4-35
Module Information Dialog Box 5-14
Gigabit Ethernet Module Physical Port Configuration Dialog Box 5-15
Detailed Port Configuration Window 5-16
Module Information Dialog Box 5-19
Physical Port Configuration Window for the Fast Ethernet Module installed in Slot 6 (partial view) 5-20
Detailed Physical Port Configuration Window 5-21
Module Information Dialog Box 5-26
Physical Port Configuration Dialog Box 5-27
All Module Ports Configuration Dialog Box 5-27
Switch Ports Dialog Box 5-28
Switch Port Configuration Dialog Box 5-31
Module Information Window 5-38
Switch Ports Dialog Box 5-39
Physical Port Configuration Dialog Box 5-41
All Ports Configuration Dialog Box 5-42
Address Forwarding Table Configuration Dialog Box 6-2
Address Table Instance Dialog Box 6-5
Address Entry Search Dialog Box. 6-9
Address Forwarding Table Dialog Box 6-10
Static Address Configuration Dialog Box. 6-13
Layout of the Redundant Backplane 7-2
Default Hardware Configuration 7-4
Switch Fabric Status Dialog Box 7-5
Switch Fabric Status Dialog Box 7-7

CPU Redundancy Configuration Window 7-9
CPU Redundancy Status 7-10
DNS Configuration Dialog Box 8-2
RADIUS Dialog Box. 8-4
IP Interfaces Dialog Box 9-2
Add IP Interface Dialog Box. 9-5
IP Global Configuration Dialog Box. 9-8
Multinet Diagram 9-13
IP Access List Dialog Box 9-15
Create IP Standard Access List Dialog Box 9-15
IP Extended Access Rule Creation Dialog Box 9-17
IP Access Control Dialog Box 9-23
IP Static ARP Entries Dialog Box 9-25
Add IP Static ARP Entry Dialog Box 9-25
IP BOOTP/DHCP Server Dialog Box 9-26
Add BOOTP/DHCP Server Entry Dialog Box 9-27
IP Global Configuration Dialog Box 9-29
IGMP Global Configuration Dialog Box 9-30
IGMP Interfaces Dialog Box 9-31
DVMRP Global Configuration Dialog Box 9-34
DVMRP Interfaces Dialog Box 9-36
IP Routing Global Statistics Dialog Box 9-39
IP Route Table Search Dialog Box 9-44
IP Route Table Dialog Box 9-46
IP Route Table Statistics Dialog Box 9-46
ARP Cache Entry Search Dialog Box 9-47
IGMP Global Statistics Dialog Box 9-49
IGMP Interface Statistics Dialog Box 9-50
DVMRP Global Statistics Dialog Box 9-55
DVMRP Interface Statistics Dialog Box 9-56
DVMRP Route Table Statistics Dialog Box 9-59
DVMRP Route Table Dialog Box 9-60
Designated Forwarder(s) Table Dialog Box 9-62
IP Global Configuration Dialog Box 9-68
IP Interface Dialog Box 9-69
VRRP Virtual Routers Dialog Box 9-70
Add VRRP Virtual Router Dialog Box 9-71
VRRP Virtual Router Statistics Dialog Box 9-72
ICMP Router Discovery Protocol Dialog Box 9-75
LDAP Configuration Dialog Box 9-78
LDAP Statistics Dialog Box 9-80
IP Static Routes Dialog Box 9-82
Add IP Static Routes Dialog Box 9-82
Add IP Interface Dialog Box 9-84
RIP Global Configuration Dialog Box 10-2
RIP Interfaces Dialog Box 10-3

RIP Trusted Neighbors Dialog Box 10-6
Add Trusted RIP Neighbors Dialog Box 10-7
RIP Interface Statistics Dialog Box 10-7
OSPF Global Configuration Dialog Box 11-2
OSPF Areas Dialog Box 11-4
ADD OSPF Area Dialog Box 11-4
OSPF Interfaces Dialog Box 11-7
OSPF Virtual Links Dialog Box 11-9
Add OSPF Virtual Link Dialog Box 11-10
OSPF Summaries Dialog Box 11-13
Add OSPF Summary Dialog Box 11-14
OSPF Statistics Dialog Box 11-17
OSPF Links Dialog Box 11-19
OSPF Neighbors Dialog Box 11-20
Link State Database Search Dialog Box 11-23
OSPF Link State Database Dialog Box 11-25
LSA Detail Dialog Box 11-26
IPX Datagram in Detail 12-2
IPX Global Configuration Dialog Box 12-4
IPX Interfaces Dialog Box 12-6
Add IPX Interface Dialog Box 12-7
IPX Static Routes Dialog Box. 12-9
Add IPX Static Route Dialog Box 12-10
IPX Static Services Dialog Box 12-13
Add IPX Static Service Dialog Box 12-13
IPX Global Statistics Dialogue Box 12-17
IPX Route Table Search Dialog Box 12-19
IPX Route Table Statistics Dialog Box 12-21
IPX Service Table Search Dialog Box 12-22
IPX Service Table Statistics 12-24
IPX RIP Interfaces Dialog Box 13-1
IPX RIP Filters Dialog Box 13-3
Add IPX RIP Filter Dialog Box 13-4
IPX SAP Interfaces Dialog Box 14-1
IPX SAP Name Filters Dialog Box. 14-4
Add IPX SAP Name Filter Dialog Box 14-5
IPX SAP Net Filters Dialog Box 14-8
Add IPX SAP Net Filter Dialog Box 14-8
IPX SAP Interface Statistics Dialog Box 14-12
AppleTalk Routing Global Configuration Window 15-3
AppleTalk Interfaces Dialog Box 15-4
Add AppleTalk Interfaces Dialog Box 15-5
Edit AppleTalk Zone Dialog Box 15-8
AppleTalk Interfaces Dialog Box 15-9
AppleTalk Static Route Dialog Box 15-10
Add AppleTalk Static Route Dialog Box 15-10

AppleTalk NBP Filter Dialog Box 15-14
Add AppleTalk NBP Filter Dialog Box 15-14
Add/Delete Interface to NBP Filter Dialog Box 15-17
AppleTalk Zone Filter Dialog Box 15-18
Add AppleTalk Zone Filter Dialog Box 15-19
Add/Delete Interface to Zone Filter Dialog Box 15-21
AppleTalk Global Statistics Dialog Box 15-23
AppleTalk Interface Statistics Table 15-26
AppleTalk Route Table Window 15-27
AppleTalk Route Table Statistics Dialog Box 15-29
AppleTalk ARP Cache Table 15-30
AppleTalk Zone Table 15-32
AppleTalk Zone Table Statistics Table 15-33
Intelligent Multicasting Global Configuration Dialog Box 16-5
Router Port Display/Configuration Dialog Box 16-7
Intelligent Multicast Session Search Dialog Box 16-10
Multicast Sessions Dialog Box 16-11
Static Multicast Sessions Dialog Box 16-14
Static Multicast Session Configuration Dialog Box 16-15
Static Multicast Sessions Dialog Box 16-16
Static Multicast Sessions Clients Port Dialog Box 16-17
IGMP Snooping Dialog Box 16-19
LGMP Server Configuration Dialog Box 16-22
LGMP Server per VLAN Dialog Box. 16-26
LGMP Client Configuration Dialog Box 16-29
LGMP Client Display per VLAN Dialog Box 16-31
CGMP Snooping Dialog Box 16-33
Temperature System Dialog Box (Layer 2) 17-3
Temperature System Dialog Box (Layer 3) 17-3
Active Alarm Table Dialog Box 17-6
General Event Management Dialog Box
(Partial View) 17-8
Protocol Event Management Dialog Box 17-9
Event Log Search Dialog Box 17-10
Shutdown Log Search Dialog Box 17-10
Event Log Dialog Box 17-11
Event Statistics Dialog Box 17-13
Layer-3 Forwarding Cache Configuration Dialog Box 18-2
Frame Forwarding Statistics Dialog Box 18-5
Route Cache Entry Search Dialog Box 18-7
FE Cache Dialog Box 18-10
Module Statistics Dialog Box 19-2
Port Statistics Dialog Box 19-2
Ethernet Interface Statistics Dialog Box 19-3
Port Mirroring Information Dialog Box 19-8
Port Mirroring Configuration Dialog Box 19-9

Module Information Dialog Box 20-3
Buffer Management Dialog Box 20-3
Buffer Detail Configuration Dialog Box 20-5

Preface

Overview of the Contents

This guide explains how to configure and operate the Cajun™ P550R®/P880/P882 switches. These switches support both layer 2 and layer 3 functionality. Also included is information on downloading new operational code to your switch. For detailed information on the command line interface, refer to *Cajun™ Command Line Interface Reference Guide*.

This guide is divided in to the following eight volumes:

Volume 1:

- **Chapter 1, Introduction to the Cajun P550R/P880/ P882 Switch** — Provides an overview of hardware and software used on all three switches.
- **Chapter 2, Initialize and Setup the Cajun P550R/P880/ P882 Switch** — Explains how to initially configure all three switches, and create users, configure protocols, manage configuration files, and configure the switches for dial-up networking.
- **Chapter 3, Configuring System Information —** Explains how to view and configure switch information such as system clock settings, and temperature, power, and cooling statistics.

Volume 2:

- **Chapter 4, Using VLANs, Spanning Tree, Hunt Groups, a nd VTP Snooping** — Provides detailed information on how to create and configure VLANs, Spanning Tree, Hunt groups, and VTP Snooping on your switch.
- **Chapter 5, Configuring Port Parameters —** Explains how to configure physical port and switch port parameters on your switch.

- **Chapter 6, Managing Address Forward Tables** — Provides information on how to configure and manage the address forwarding tables in your switch.

Volume 3:

- **Chapter 7, Configuring Redundancy Options** — Explains how to install, enable and configure redundancy hardware options on your switch.
- **Chapter 8, Configuring Domain Name System (DNS) and Remote Authentication Dial-In User Service (RADIUS) Clients** — Explains how to configure DNS and and RADIUS clients on your switch.

Volume 4:

- **Chapter 9, Configuring IP Routing** — Explains how to configure your switch for IP routing and interpret IP routing statistics.

Volume 5:

- **Chapter 10, Configuring IP Routing Interface Protocol (RIP) Routing** — Explains how to configure IP RIP on your switch.
- **Chapter 11, Configuring the Open Shortest Path First (OSPF) Routing Protocol** — Explains how to configure OSPF routing protocol on your Cajun Switch. Also provided is information on OSPF statistical displays.
- **Chapter 12, Configuring IPX Routing** — Explains how to configure IPX on your switch.
- **Chapter 13, Configuring IPX RIP Protocol** — Explains how to configure IPX RIP protocol on your switch.
- **Chapter 14, Configuring IPX Service Advertisement Protocol (SAP)** — Explains how to configure IPX SAP on your switch.

Volume 6:

- **Chapter 15, Configuring AppleTalk Routing** — Explains how to configure AppleTalk parameters and view AppleTalk statistics.
- **Chapter 16, Managing Intelligent Multicasting** — Explains how to configure and manage intelligent multicast sessions on your switch.

- **Chapter 17, Monitoring the Cajun Switch** — Explains how to use the Web Agent to assess your switch's current operational status.
- **Chapter 18, Monitoring and Configuring the Forwarding Cache (L3 Only) —** Explains how to interpret and monitor forwarding operations that occur in the address cache of the multilayer media modules**.**
- **Chapter 19, Analyzing Network Performance Using RMON and Ethernet Statistics** — Provides information on how to interpret the statistics counter values displayed in your switch.
- **Chapter 20, Tuning Your Switch Performance** — Explains how to use your switch's buffer management features to optimize traffic throughput through the switch fabric.

Volume 7:

- **Appendix A, Downloading New Operational Code to the Switch** — Explains how to update the operational code on your switch.
- **Appendix B, Boot Mode** —
- **Appendix C, MIB Groups** — Provides information on the supported MIB groups.
- **Appendix D, FCC Notice** — Provides the FCC notice statement.

Volume 8:

- **Index**

Technical Support

To contact Avaya's technical support:

- From the United States and North America:

  Dial

  - 1-800-237-0016
  - 1-800-242-2121

- Outside North America:

  Contact your distributor

Avaya Technologies Products and Services

Refer to the Avaya World Wide Web site at:

http://www.Avaya.com/dns.

for information about Avaya products and services.

Conventions

The following conventions are used throughout this guide::

Convention	Represents	Examples
User Input	User entered text.	To create a new password, type `store password root`
Boldface Text	Represents a menu command, a keyword to be acted upon, or a button name.	Select **Default** from the **Interface** pull-down menu. Click **Cancel** to stop the installation.
System Output	Text displayed by the system.	If you attempt the find the physical location of port 30, the system displays `Unit 2 Port 2`
+ or -	Expand or collapse a navigation tree folder.	To set your server location, you must first expand the System folder, then expand the Configuration folder to see the Server Location link.
Using the Web Agent.	The Web Agent consists of folders that you must open to perform a specific operations. The folders are part of a group located on the web agent window.	Select Modules & Ports from the System>Configuration group on the web agent window.

Convention	Represents	Examples
The words '**Select**' and '**Click**'.	In this guide: **Select** means to point and click on a specific item that then opens another dialog box, window, option box, etc.. **Click** means to point to an action and press the left mouse button once to perform an operation.	 **Select** Modules & Ports from the **System>Configuration** group on the web agent window. The Module Configuration dialog box opens. **Click** Apply to accept the change, or Cancel to ignore the change
Web Agent vs. Command Line Interface (CLI) steps.	The procedures in this guide provide detailed steps from the Web Agent. A series of CLI commands are also available that accomplish the same actions. These commands are listed after the web agent procedure followed by a reference to the *CLI Reference Guide* for more detailed information.	Select the port number for a module from the Ports column. The CLI command is show port (mod-num> (refer to the *Cajun Switch CLI Reference Guide* for more detailed information).
Knowledge level	Allof the procedures in this guide are written assuming that the audientc knows how to maneuver through a windows-type environment (use scoll bars, open pull-down menus, etc.).	Scroll to the "Configuring IP Using the Web Agent" section. Open the In-band IPC pull-down menu.

Using Notes, Cautions, and Warnings

The following text and icon conventions are used in this guide for Notes, Cautions, and Warnings.

*** Note:** Provides additional information about a procedure or topic.

WARNING

Indicates a condition that *may cause* bodily injury or death.

CAUTION

Indicates a condition that *may damage* hardware or software.

Related Documentation

This section provides information on supporting documentation, including:

- Online Documentation
- Documentation
- Terminology

Online Documentation

Avaya Technologies maintains copies of technical documentation on the corporate web server. To access online documentation, including HTML and PDF documents, use Netscape Navigator® version 4.5 or higher or Microsoft® Internet Explorer version 3.x or higher and enter the following URL:

```
http://pubs.Avayactc.com/
```

Online Help

You must have a browser installed on your system in order to use the on-line help.

*** Note:** If you are using Netscape®, use version 4.5 or later. Also, you must configure the Proxies to:

Direct Connection to the Internet.

Open:

Edit > **Preferences** > **Advanced** > **Proxies**

and verify that the **Direct Connection to the Internet** button is selected.

When launching the online help, wait until the help window has completely loaded before resizing the window.

Installing Online Documentation and Help Files

You can access Online documentation and help files used by the Web Agent by either:

- Installing the HTTP documentation server (available on the Avaya user documentation CD, CajunDocs)
- Adding the files to an existing web server on your network

You must set up the HTTP documentation help server for the switch. This allows the switch to access:

- Online documentation
- Bitmaps used as part of the interface (logo, wallpaper)
- Online help files for the Web Agent

Installing the HTTP Documentation Server

You can access online documentation and help files directly from the HTTP documentation server. The server must be running a Win32 compatible operating system (for example, Windows 95, Windows 98, or Windows NT).

To install the HTTP documentation server:

- Run the **Setup** program from the CajunDocs CD-ROM

Or

- Go to the Avaya Publications web site (**http://pubs.Avaya.com/CD-ROM/cajundocs.html**) and select the latest released version of the CajunDocs CD. Run the **Setup** program (setup.exe). This extracts the help server and the online help system.

Starting the HTTP Web Server

To run the HTTP help server:

1. Open you system's (Wind32/NT) Start Menu.
2. Select the **CajunDocs** program group.
3. Select the document server from that program group.

The Avaya document server will launch. To access this server from a Web browser you need to set a server location on the switch, as explained in "Entering the Server Location on the Switch" section.

Entering the Server Location on the Switch

To set the location of the documentation server:

1. Launch your Web browser and connect to your switch.
2. Enter your **user name** and **password** at their respective prompts and select OK.
3. Select **Server Location** from the **System Configuration** group. The **Online Help Configuration** dialog box opens.

4. Enter the **host name** or **IP address** followed by the port designation of *:2010* for the HTTP server in the **HTTP Server Location** field (for example, the correct syntax for host named phantom is: `http://phantom:2010`).

   *** Note:** The default port number for HTTP is port **80**. The default port number for telnet is **23**.

   If you decide to install your online help on a Web server other than the HTTP server bundled on the CajunDocs CD-ROM, you can specify the URL without a port number if your Web server runs on port 80 (for example, `http://www.abc-company.com`).

5. Select **Apply** to accept the server location you entered or cancel to ignore the location.

Adding Document Files to an Existing Server

You can install the online help to a Web server other than the HTTP server bundled on the CajunDocs CD-ROM. You must transfer the help subdirectory to that Web server and enter the URL for that web server in the **Server Location** field.

To transfer the CajunDocs help directory to your company server (http://www.abc-company.com):

1. Install the online help and documentation from the CajunDocs CD to a Windows95 or NT node on your network.
2. Transfer the entire help subdirectory located in **C:\CajunDocs** to the root directory of your Web server.
3. Launch your web browser and connect to your switch.
4. Enter your **user name** and **password** at the respective prompts and select OK.
5. Select **Server Location** from the **System Configuration** section. The **Online Help Configuration** dialog box opens.
6. Enter the **server location** in the **HTTP Server Location** field (for example, http://www.abc-company.com).

7. Enter the **directory name** of your help files in the **HELP Directory Location** field. For example, **help**.

*** Note:** The default for the help directory is **help**. You do not need to change this unless you changed the name of your help directory.

8. Select **Apply** to accept the HTTP Server Location you entered or cancel to ignore the location.

Downloading an Updated CajunDocs CD from the Internet

The server and help files are available on the Internet. To download updated files from the Internet to your CajunDocs CD directory:

1. Launch a web browser.
2. Go to the **CajunDocs Installer** Web page at:

   http://pubs.Avayactc.com/cdrom/cajundocs.html

3. Download the latest version of the CajunDocs CD-ROM installer to the directory you previously created.

For more information on this product, refer to the online documentation that comes on your CajunDocs CD-ROM or refer to http://pubs.Avayactc.com to review the online documentation there.

Documentation

The following documents provide additional information on Avaya products:

- *Cajun P550R/P880/P882 Installation Guide* describes how to install and set up the family of Cajun switches.
- *Cajun P550R/P880/P882 Switch User Guide* describes how to operate, configure, and maintain the family of Cajun P550R/P880/P882 switches.

Terminology

Throughout this guide, the term **Layer 2**, is used to indicate switching capabilities. For example, **Layer 2 Supervisor Module,** indicates a supervisor module that enables switching.

The term, Layer 3 refers to the combined ability to switch and route. For example, the name, **Layer 3 supervisor module,** indicates a supervisor module that provides switching and routing capabilities.

Documentation Feedback

If you have comments about the technical accuracy or general quality of this document please send us an email at:

techpubs@Avaya.com

Please cite the document title, part number, and page reference, if appropriate.

1 Introduction to the Cajun P550R/P880/P882 Switch

Overview

The following information and procedures are provided in this chapter:

- Switch Description
- Hardware Components
- Software Features
- Routing Overview

Switch Description

The Cajun P550R/P880/P882 switches are high performance campus Gigabit Ethernet switch for LAN backbone applications. These switches are the centerpiece for Avaya data, voice and multimedia LANs. The P550R switching capacity ranges from 46Gbps in 50-series mode to 55Gbps in 80-series mode. The P880/P882 switching capacity ranges from 56Gbps, in 50-series mode, to 139Gbps, in 80-series mode.

The switches support specific hardware components and various software features.

The Cajun switches provide the following features:

- Increased bandwidth
- Elimination of bottlenecks
- Better manageability
- Routing
- Dependable multimedia support
- Redundant switch-switch trunks (link aggregation - Hunt-Groups)

Version 5.0 software provides the following new hardware and software features:

Hardware Features:

- 80-Series Module Support

Software features:

- Domain Naming System (DNS) Client Support
- Remote Authentication Dial-In User Service (RADIUS) Client Support
- Load MIB Support
- Open Shortest Path First (OSPF) Passive Interface support

Hardware Components

The Cajun switch provides the following hardware components:

- Chassis
- 50-Series Modules
- 80-Series Modules

Chassis

The Cajun switch chassis comes in two models:

- The P550R chassis
- The P880/P882 Chassis.

Each chassis can run in two modes:

- 50-series mode
- 80-series mode

50-Series Mode

The 50-series platform offers a switching fabric performance if 1.76 gigabit per second per fabric port. 50-series modules operate at 55MHz only. The presence of any 50-series modules within the chassis will cause the chassis to operate in 50-series mode.

In 50-series operation the P550R chassis will have a 13x13 crossbar switching fabric, while the P880/P882 chassis will have a 16x16 cross bar switching fabric. In addition, the P880/P882 chassis is limited to sixteen functional slots in 50-series mode (slot 17 can not be used).

80-Series Mode

The 80-series platform is an evolution of the 50-series architecture. It offers 20% increase in switching fabric performance or 2.11 gigabit per second per fabric port. This allows larger 10/100/1000 port density on a per crossbar port basis.

This increase in performance is accomplished with new Cajun ASICs that operate at 66MHz (as well as 55MHz capable) and consolidate as well as enrich the functionality of a number of ASICs currently used in the 50-series modules.

This increased performance can only occur if the entire switch contains 80-series modules. The presence of any 50-series modules within the chassis will cause the chassis to operate in 50-series mode.

In 80-series operation the P550R chassis will have a 13x13 crossbar switching fabric, while the P880/P882 chassis will have a 31x31 cross bar switching fabric.

P550R Chassis

The Cajun P550R Chassis consists of:

- Seven slots (1 slot for the supervisor module and six payload slots for media modules)
- Fan Tray
- Increased port density
- Up to three power supplies
- A 13x13 crossbar switch fabric

Slots

The P550R chassis consists of seven slots. Slot 1 is dedicated for a supervisor module and the remaining six of which are payload slots. If a redundant supervisor is used in the chassis, it must be inserted into slot 2 of the chassis.

Ports

The P550R chassis configured with 50-series modules provides support for:

- Up to 120 10/100BASE-TX ports (RJ-45 connector, autosensing)
- Up to 288 10/100BASE-TX ports (Telco connector, autosensing)
- Up to 60 100BASE-FX ports
- Up to 24 gigabit-speed Ethernet ports

With 80-Series modules, the P550R chassis provides support for:

- Up to 144 10/100BASE-TX ports (RJ-45 connector, autosensing)
- Up to 288 10/100BASE-TX ports (Telco connector, autosensing)
- Up to 144 100BASE-FX ports (MJRT connector)
- Up to 48 gigabit-speed Ethernet ports

Fan Tray

There are two fan assemblies in the chassis. One fan assembly is located on the left side of the chassis to provide air flow to the media modules installed. This fan assembly is hot-swappable. The other fan assembly is located in the rear of the chassis to provide air flow to the switch fabric. This fan assembly is not field replaceable.

Power Supplies

Only two power supplies are required to support a fully-loaded P550R chassis. A third power supply can be installed to provide backup should one of the other two fail.

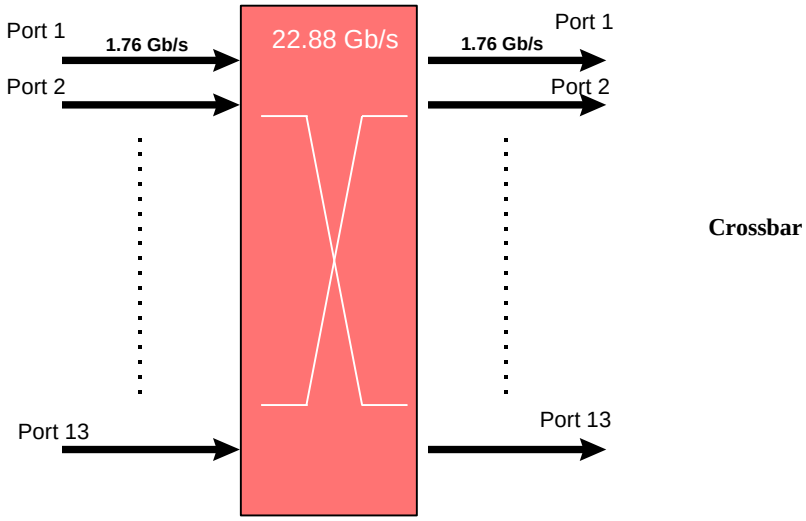
The power subsystem provides N+1 power supply redundancy. In addition, the installed power supplies will load share between the installed units. The power supplies are also warm swappable (power supplies must be turned off and unplugged before removing them from the chassis, however the other power supplies can remain on).

Switch Fabric

In 50-Series mode, the switching fabric provides 22.88 Gbps switching throughput (45.76 Gbps aggregate bandwidth). In 80-Series mode, the switching fabric provides 27.455 Gbps switching throughput (54.91 Gbps aggregate bandwidth).

The crossbar switch matrix provides low latency, high throughput packet switching using a crossbar architecture (Figure 1-1).

Figure 1-1. Crossbar Architecture



Crossbars are inherently more scalable than shared memory architectures. You can add more capacity simply by adding more switch elements. By comparison, shared memory switches have an inherent maximum upper boundary in throughput that makes high-density, single-backplane gigabit switches impractical. This means that as you increase the number of gigabit ports in your network, the architecture can scale to meet your needs.

The crossbar supports:

- 13 fabric ports (two per I/O module slot, one for the supervisor module).
- 1.76 GB/s (in and out) on each fabric port in 50-series mode and 2.11 GB/s (in and out) on each fabric port in 80-series mode.
- 22.88 GB/s total capacity, 45.76 GB/s total backplane capacity in 50-series mode and 27.455 GB/s total capacity, 54.91 GB/s total backplane capacity in 80-series mode.
- Under-subscribed switching fabric in most configurations (two connections per I/O module slot, plus one for the supervisor module).
- Single copy replication - Input frames that are destined for output multiple switch ports pass through the crossbar only once and are copied by the crossbar to each destination.
- Hardware-assisted multicast pruning - The switch only forwards to appropriate destination switch ports.

P880/P882 Chassis

The P880/P882 Chassis consists of:

- Seventeen slots (1 slot for the supervisor module and sixteen payload slots for media modules)
- Fan Tray
- Increased port density
- Up to three power supplies
- A 33x33 crossbar switch fabric

Slots

The P880/P882 chassis consists of seventeen slots. Slot 1 is dedicated for a supervisor module and the remaining sixteen of which are payload slots.

In 50-series mode, the P880/P882 Chassis can only support up to 15 payload slots. Slot seventeen is unsupported in 50-series mode. In 80-series mode, all sixteen payload slots are usable.

If a redundant supervisor is used in the chassis, the redundant supervisor must be inserted into slot 2 of the chassis

Ports

With 50-Series modules, the P880/P882 Chassis provides support for:

- Up to 120 10/100BASE-TX ports (RJ-45 connector, autosensing)
- Up to 288 10/100BASE-TX ports (Telco connector, autosensing)
- Up to 60 100BASE-FX ports
  - Up to 24 gigabit-speed Ethernet ports

With 80-Series modules, the P880/P882 chassis provides support for:

- Up to 38410/100BASE-TX ports (RJ-45 connector, autosensing)
- Up to 76810/100BASE-TX ports (Telco connector, autosensing)
- Up to 284100BASE-FX ports (MJRT connector)

- Up to 128 gigabit-speed Ethernet ports

Fan Tray

There are two fan assemblies in the chassis. One fan assembly is located on the left side of the chassis to provide air flow to the media modules installed. The other fan assembly is located in the rear of the chassis to provide air flow to the switch fabric. Both fan assemblies are hot-swappable and field replaceable.

Power Supplies

Only two power supplies are required to support a fully-loaded P880/P882 Chassis. A third power supply can be installed to provide backup should one of the other two fail.

The power subsystem provides N+1 power supply redundancy. In addition, the installed power supplies will load share between the installed units. The power supplies are also warm swappable (power supplies must be turned off and unplugged before removing them from the chassis, however the other power supplies can remain on).

Switch Fabric

In 50-Series mode, the switching fabric provides a 16x16 crossbar that provides 28.16 Gbps switching throughput (56.32 Gbps aggregate bandwidth). In 80-Series mode, the switching fabric provides a 31x31 crossbar that provides 69.696 Gbps switching throughput (139.392 Gbps aggregate bandwidth).

The crossbar switch matrix provides low latency, high throughput packet switching using a crossbar architecture.

Crossbars are inherently more scalable than shared memory architectures. You can add more capacity simply by adding more switch elements. By comparison, shared memory switches have an inherent maximum upper boundary in throughput that makes high-density, single-backplane gigabit switches impractical. This means that as you increase the number of gigabit ports in your network, the architecture can scale to meet your needs.

The P880/P882 chassis crossbar supports:

- 31 fabric ports (two per I/O module slot, plus one for the supervisor module).
- 1.76 GB/s (in and out) on each fabric port in 50-series mode and 2.16 GB/s (in and out) on each fabric port in 80-series mode.
- 28.16 GB/s total capacity, 56.32 GB/s total backplane capacity in 50-series mode and 56.32 GB/s total capacity, 139.392 GB/s total backplane capacity in 80-series mode.

- Under-subscribed switching fabric in most configurations (two connections per I/O module slot, plus one for the supervisor module).
- Single copy replication - Input frames destined for output multiple switch ports pass through the crossbar only once and are copied by the crossbar to each destination.
- Hardware-assisted multicast pruning - The switch only forwards to appropriate destination switch ports

50-Series Modules

The Cajun P550/P880/P882 switches support the following 50-Series modules:

- Layer 2 Supervisor Module
- Layer 3 Supervisor Module
- Layer 2 and Layer 3 Fast Ethernet Modules
- Layer 2 and Layer 3 Gigabit-Speed Modules
- ATM Uplink Module

The layer 2 and layer 3 media modules implement wire speed routing and bridging in Application-Specific Integrated Circuits (ASICs). One set of ASICs supports a gigabit-per-second's worth of traffic (any combination of layer 2 and layer 3 modules). The routing and bridging ASICs can process 1.5 million packets per second, which is just slightly more than a gigabit's worth of minimum-sized Ethernet frames.

*** Note:** All layer 3 modules interoperate with the layer 2 modules and require the layer 3 supervisor module.

The layer 2 and layer 3 supervisor modules are both responsible for learning addresses, and managing the address cache and the Spanning Tree Protocol (STP).

The ATM Uplink module provides LAN Emulation (LANE) connectivity over an ATM network.

Layer 2 Supervisor Module

The layer 2 supervisor module provides the following features:

- Learns addresses

- Manages the address cache and the Spanning Tree Protocol (STP)
- PowerPC 860 RISC processor
- Memory: 4 MB Flash, 8 MB DRAM, 128 KB NVRAM
- Multiple memory configurations (Table 1-1):

Table 1-1. Multiple Memory Configuration

DIMM/SIMM	Number of Modules	Total Memory
8 MB	1	8 MB
16 MB	1	16 MB
32 MB	1	32 MB

- Real-time clock
- Out-of-band console: 10BASE-T & RS-232
- RMON support
- SNMP management agent
- Dot matrix display

Layer 3 Supervisor Module

The layer 3 Supervisor module requires a faster CPU and more memory. Also, unlike the layer 2 supervisor, the layer 3 supervisor is part of the path that some packets take through the system. To accomplish this, the layer 3 supervisor requires faster data transfer to and from the switching fabric.

The layer 3 supervisor module features are:

- PowerPC 750 (RISC) processor
- Memory: 4 MB Flash, 64 MB DRAM, 128 KB NVRAM, 512 KB cache
- Multiple memory configurations (refer to Table 1-2)

Table 1-2. Multiple Memory Configuration

DIMM/ SIMM	Number of Modules	Total Memory
32 MB	1	32 MB
32 MB	2	64 MB

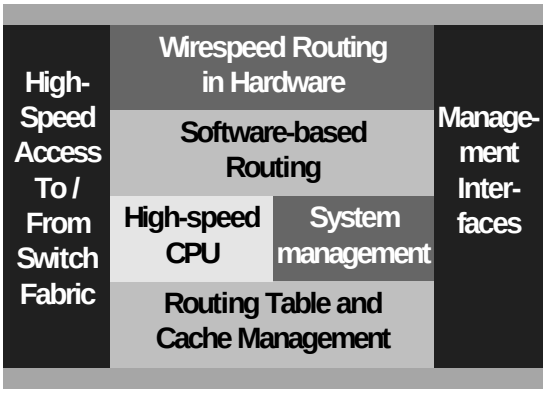
Table 1-2. Multiple Memory Configuration

DIMM/ SIMM	Number of Modules	Total Memory
64 MB	1	64 MB
64 MB	2	128 MB

- Real-time clock
- Out-of-band console: 10/100BASE-T & RS-232
- RMON support
- Simple Network Management Protocol (SNMP) support
- Dot matrix display
- System management functions and interfaces
- Routing protocols tables and caches
- 1.5 million packets per second of hardware-based routing for packets that arrive on layer 2-only media modules
- Software-based routing for packets that are not routed in hardware
- Implementation of layer 3 data forwarding for protocols, such as AppleTalk, that are not implemented in hardware
- PCMCIA interface that only supports the Flash card that you can order from Avaya.

Figure 1-2 illustrates a conceptual diagram of the layer 3 supervisor module's functions.

Figure 1-2. Layer 3 Supervisor Conceptual Operation



Multilayer Supervisor Conceptual Diagram

Redundant Supervisor

The redundant supervisor module is an auxiliary (standby) supervisor module that acts as a fault-tolerant supervisor in the event that your active supervisor fails. The redundant supervisor provides a seamless solution to switch failure. Once the redundant supervisor is installed, loaded with the same software version as the active supervisor, and synchronized, it is ready to act as a backup to the active supervisor. If the active supervisor does fail, the redundant module quickly assumes control with the least possible affect on network operation. No user intervention is required for the CPU module switchover. The management view is accessible without changing IP or MAC addresses. The switch version (ver) is logged and indicated via an SNMP trap.

The redundant supervisor introduces the concepts of an internal network and internal network mask.

The internal IP network consists of an internal network Virtual LAN (VLAN) that is only used to connect the redundant supervisors in slots 1 and 2. Health messages get passed and image and configuration synchronization access between the supervisor modules are done over the internal IP network. The internal IP network uses the internal network IP mask.

The slot specific Ethernet console IP address is an additional IP address that is always assigned to the supervisor modules in slot 1 and slot 2, regardless of whether the supervisor module slot 1 is active or standby. always use this address if you want to access the supervisor module in either slot.

The firmware in initial versions of the P550 layer 2 supervisor (model M5500-SUP-8) does not fully support redundant supervisors. The supervisor module will report the following message to the console port and the LED banner when it is installed in a chassis with a second supervisor:

If redundant supervisor modules are required in your switch, then the supervisor module(s) that report this message must be upgraded. To get the upgrade, please contact:

Avaya CTC RMA Department:

Phone: 800-950-7925 ext. 9532

e-mail: rma@Avayactc.com

If you installed a second supervisor module in slot 2 in your switch, but do not require redundant supervisor operation, you can remove

the supervisor module from slot 2 and restart your switch. There is no need to upgrade the firmware if you are not running redundant supervisors.

*** Note:**

- 16 MB of memory is required on layer 2 supervisor modules. If you have a P550 switch and the supervisor module is not configured with 16 MB of memory, you should order one of the following upgrades:

  Model M5500-MEM16 for 16 MB upgrade

  Or

  Model M5500-MEM32 for 32 MB upgrade

Media Modules

All of the *layer 3 media modules* have the same general function as the layer 3 supervisor module except for the following:

- The number and type of physical interfaces
- Hardware-based routing and bridging capacity

Bridging and routing are performed on the input side of each media module. Frames whose destination Media Access Control (MAC) address is on the same Virtual LAN (VLAN) as the interface on which they arrived are bridged. Frames that are going from one VLAN to another are routed. Some frames are both bridged and routed, as is the case with multicast.

The media module's features include:

- **IEEE 802.3x full-duplex flow control -** This allows the switch ports to send a pause command before input buffers overflow. Half-duplex ports support active backpressure (jamming).
- **VLAN trunking or non-tagged access modes -** This allows the switch ports to interoperate with popular tagged trunking schemes used by large networking vendors.
- **Priority Queuing and Class of Service -** These features allow you to prioritize traffic between particular stations or sets of stations to support jitter-sensitive applications. Supported class of service (CoS) types include the following:

  — 3COM PACE CoS

- IEEE 802.1p CoS
- Layer 3 tagging

Layer 2 and Layer 3 Fast Ethernet Modules

All three switches support the following layer 2 and layer 3 Fast Ethernet modules:

- 20-Port 10/100BASE-TX Ethernet module (layer 2 support), with 20 RJ-45 Ports – 10/100, HDX/FDX (M5520-100TX)
- 10-Port 100BASE-FX Ethernet module (layer 2 support), with 10 Fast Ethernet Ports – Fiber, 1300 nM, HDX/FDX (M5510-100FX)
- 48-Port, 10/100BASE-TX Ethernet module (layer 3 support), with 48 RJ-71 Ports – 10/100, HDX/FDX
- 10-Port 100BASE-FX Ethernet module (layer 3 support), with 10 Fast Ethernet Ports – Fiber, 1300 nM, HDX/FDX (M5510R-100FX)
- 12-Port 10/100BASE-TX Ethernet module (layer 2 and layer 3 support), with 12 RJ-45 Ports – 10/100, HDX/FDX (M5512R-100TX)

Layer 2 and Layer 3 Gigabit-Speed Modules

All three switches support the following layer 2 and layer 3 Gigabit Ethernet modules:

- 2-Port, Full-Duplex 1000BASE-SX module (layer 2 support) 850 nM optics (M5502-1000SX-F)
- 2-Port, Full-Duplex 1000BASE-LX module (layer 2 support) 1300 nM optics (M5502-1000LX-F)
- 2-Port, Full-Duplex 1000BASE-SLX module (layer 2 support) 10 Km with 1300nM optics (M5502-1000SLX-F)
- 4-Port, Full-Duplex 1000BASE-SX-F module (layer 2 and layer 3 support) 850 nM optics (M5504-1000SX-F)
- 2-Port, Full-Duplex 1000BASE-SX-F module (layer 2 and layer 3 support) 850 nM optics (M5502R-1000SX-F)
- 2-Port, Full-Duplex 1000BASE-LX-F module (layer 2 and layer 3 support) 1300 nM optics (M5502R-1000LX-F)

ATM Uplink Module

There are four variations of the ATM Uplink module:

- 2 port Synchronous Optical NETwork (SONET)/ Synchronous Digital Hierarchy (SDH)) OC-3c/STM-1 Single Mode Fiber (SMF)
- 2 port SONET/SDH OC-3c/STM-1 MMF (MultiMode Fiber)
- 2 port SONET/SDH OC-12c/STM-4c SMF
- 2 port SONET/SDH OC-12c/STM-4c MMF

Each module has multiple physical interfaces that are capable of being simultaneously active.

The major features of the ATM Uplink module are:

- LANE V2 Client - with LANE 1 compatibility, supports 128 interfaces
- QoS (Quality of Service) support for UBR, nrt-VBR, rt-VBR, and CBR
- ATM UNI (User-to-Network Interface) V 3.0, 3.1and 4.0 signaling
- ILMI (Integrated Local Management Interface) Version 4.0
- PNNI (Private Network - to - Network Interface) non-transit
- Link Failover
- Spanning Tree

*** Note:** All ATM protocols are ATM Forum standard.

Refer to the *Cajun P550/P550R Switch ATM Uplink Configuration Guide* for more detailed information.

80-Series Modules

All three switches support the following 80-Series modules:

- 4-port, Gigabit Interface Card (GBIC) based module — This module can be configured with up to 2 GBIC optical modules. It has two switch ports to the backplane providing more than two Gb per second bidirectional data traffic to the switch. This module can support the following GBIC-type connectors:
  - 850 nM multimode (1000BASE-SX)
  - 1300 nM singlemode (1000BASE-LX)

— 1550 nM singlemode (1000BASE-ELX)

*** Note:** If you use the 1000BASE-SX GBIC with single mode fiber, you must use mode conditioning patch cords with a maximum distance of 500m.

- 8-port, GBIC based module — This module can be configured with up to 4 GBIC optical modules. It also has two switch ports to the backplane that provide more than two Gb per second bidirectional data traffic to the switch. There are four GBICs per port each capable of one Gb per second. Each GBIC has an oscillated GQ, F-chip, and packet and lookup memories.

  The 8-port GBIC module can support the following GBIC-type connectors:

  — 850 nM multimode (1000BASE-SX)

  — 1300 nM singlemode (1000BASE-LX)

  — 1550 nM singlemode (1000BASE-ELX)

  *** Note:** If you use the 1000BASE-SX GBIC with single mode fiber, you must use mode conditioning patch cords with a maximum distance of 500m.

- 24-Port 10/100BASE-TX Ethernet module (layer 2 and layer 3 support), with 12 RJ-45 Ports – 10/100, HDX/FDX (M5512R-100TX)
- Layer 3 Supervisor Module with PCMCIA

Software Features

All three switches support the following software features:

- Virtual Bridging Functions
- Flood Pruning Using VLANs
- Hunt Groups
- OpenTrunk Technology
- Domain Naming System (DNS) Client Support
- Remote Authentication Dial-In User Service (RADIUS) Client Support
- OSPF Passive-Interface Support

- Load MIB
- Spanning Tree Modes
- Buffer and Queue Management

Virtual Bridging Functions

All three switches are designed to support:

- Up to 24,000 MAC addresses in the switch address forwarding table — allows the switch to store forwarding information for hosts in very large networks.
- Segmented address tables qualified by address and VLAN membership — allows the same host to appear on different VLANs on different ports.
- Optional per-VLAN STP — isolates loop control to smaller domains, so spanning trees converge faster after a topology change. Otherwise, packets are forwarded to the port's default VLAN.

Flood Pruning Using VLANs

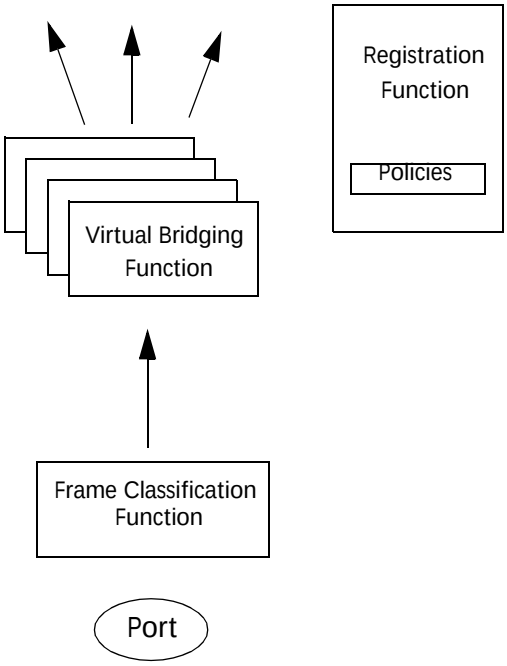
VLANs provide network managers with two significant capabilities:

- The ability to segment traffic in a flat switched network. This helps prevent traffic from being forwarded to stations where it is not needed.
- The ability to ignore physical switch locations when creating workgroups. VLANs are logical constructions and can traverse physical switch boundaries.

The hardware on all three switches support port-based VLANs with the following characteristics:

- Frames classified as Layer 1 (Port-based) when they enter the switch
- Explicitly tagged VLAN packets — these are forwarded based on the information in the packet.
- Up to 1,000 VLANs — VLANs define a set of ports in a flooding domain. Packets that need to be flooded are sent only to ports participating in that VLAN (Figure 1-3).

Figure 1-3. Flooding Domain



Hunt Groups

Hunt groups allow you to aggregate bandwidth from multiple ports so they act as one high-bandwidth switch port. Hunt groups create multi-gigabit pipes to transport traffic through the highest traffic areas of your network. You can create hunt groups that interoperate with other vendor's equipment (for example, Cisco's Etherchannel and Sun's Quad Adapter).

OpenTrunk Technology

All three switches are delivered as a plug-and-play IEEE 802.1D standard bridge, but support several VLAN tagging schemes. This makes the switch highly interoperable in existing networks because:

- Any port can be a trunk port.
- Ports have configurable VLAN tagging on a per-port basis.
- Ports process a number of popular VLAN tagging schemes, including major vendors' proprietary schemes.

The following are features of Open Trunk Technology:

- Frame encapsulation
  - Identifies frame VLAN via tag
  - Associates frame priority
- Multiple tagging formats
  - IEEE pre-standard format based on 802.1Q draft document
  - A major vendor's multi-level tagging scheme
  - 3Com VLAN Tag & PACE priority signalling
- Translation to and from any format. A packet can enter the switch with a 3Com SuperStack II VLAN tag and exit the switch as a multi-layer tagged packet.

Domain Naming System (DNS) Client Support

DNS is a distributed database of name servers which supply name-to-address translations. DNS is made up of three types of name servers:

- The root name server — Located at the top of the DNS database tree. It contains pointers to the master name servers for each of the top-level domains.
- The master name server — Located in the middle of the DNS database tree. It contains pointers to the individual name servers for each of the subdomains within its top-level domain.
- The individual name server — Located at the bottom of the DNS database tree. It contains detailed address information for the local hosts in the subdomain.

All three switches map domain names to IP addresses through DNS clients. DNS must be enabled on the switch and at least one name server IP address must be specified.

The following DNS Client features are supported:

- DNS name-to-address translation can be enabled or disabled from either the CLI or the Web Agent
- Up to six DNS name servers can be configured
- Up to six default domain name suffixes can be configured

- When DNS is enabled, DNS names can be used in place of IP addresses for `ping`, `telnet`, `connect, and traceroute and copy tftp` CLI commands
- The DNS client name can consist of up to 255 characters
- A single label within a DNS client name can consist of 63 characters
- The time to live (TTL) value in a DNS resource record is 24 days.

Remote Authentication Dial-In User Service (RADIUS) Client Support

RADIUS is a mechanism used for authenticating remote users logging into the Cajun switch. You can log into the switch in order to view or manage the switch through the CLI or the embedded web interface. A RADIUS client provides a mechanism for consolidating user login information. When a user attempts to log into the switch, if there is no local user account for the entered user name and password, then the switch will send an Authentication Request to the RADIUS server in an attempt to authenticate the user remotely. If the user name and password are authenticated, then the RADIUS server responds with an authentication acknowledgement that includes information on the user's privileges and the user is allowed access to the switch. If the user is not authenticated, then a Authentication Reject is sent to the switch and the user is denied access to the switch's embedded management.

OSPF Passive-Interface Support

OSPF passive-interface disables sending OSPF routing updates by not sending OSPF hello packets across the network. Any OSPF hello packets received from other OSPF routers on the network are also ignored. OSPF advertises the passive-interface as a stub network in the router updates it sends to other OSPF interfaces.

The OSPF passive-interface CLI commands are:

```
>passive-interface [<interface-name>|<ip-
addr>]
```

This command defines an OSPF interface as passive-interface.

```
>no passive-interface [<interface-name>|<ip-
addr>]
```

This command sets the state of an OSPF interface that is configured as a passive-interface to normal.

You can also set OSPF passive-interface from the switch Web Agent. The Interface-State field on the OSPF Interface web page can be set to Passive, which disables the sending of OSPF routing updates, or Normal, which enables the sending of OSPF routing updates (default).

Load MIB

The switch Load MIB defines upload, download and copy of application software and configuration information. The Load MIB consists of two tables:

- The genOpTable — a conceptual table where each row represents a file operation that can be performed by the switch. For example, `localConfigFileCopy` is a function that the switch software supports. Therefore, the genOpTable should always display the conceptual row representing the indicated operation.
- The genAppTable — functions as a file system directory. Each row in the genAppTable represents a file stored in ram, nvram, flash, or bootprom. By using this representation, the network management device can walk the entire genAppTable to learn what files (along with their type and location) are resident in the system.

For more detailed information, refer to Load MIB Overview in Appendix .

Spanning Tree Modes

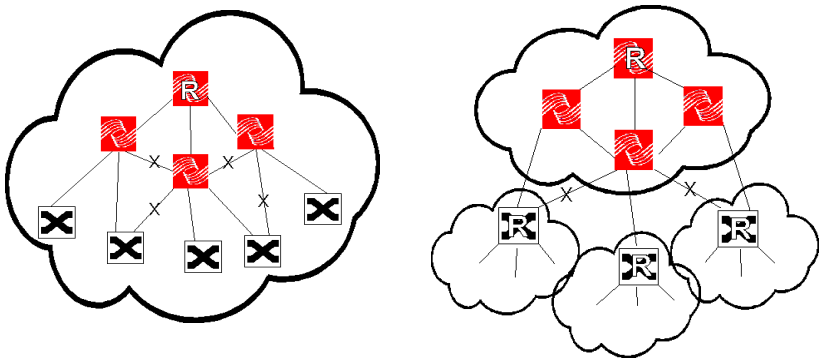
Spanning tree protocol is used to prevent loops from forming in your network. The spanning tree algorithm creates a single path through the network by ensuring that if more than one path exists between two parts of a network, only one of these paths is used, while the others are blocked.

Spanning Tree Protocol Bridge Options

All three switches support the following four Spanning Tree Protocol options:

- IEEE 802.1D Spanning Tree
- Per-VLAN Spanning Tree
- Dual-Layer Spanning Tree (Figure 1-4)
- Global Disable

Figure 1-4. Spanning Tree Models



Single 802.1D Spanning Tree
One Spanning Tree
Longer convergence
One path to and from root for all VLANs
Improper configuration
can shut down Trunk Links

Multi-Level Spanning Tree
Backbone terminates 802.1D STP
Smaller STP Domains
Quicker Convergence
VLAN Load Balancing
Interoperates w/ existing Bridge/Routers

IEEE802.1D Spanning Tree Protocol Option

All three switches participate in a Single Spanning Tree domain in the IEEE802.1D STP mode. All ports with STP configured belong to the same spanning tree domain and rules are as defined in IEEE802.1D unless otherwise specified herein. BPDUs are as defined by 802.1D and are sent out Clear on each link regardless of whether or not the link has a tagging method defined. This method is desired when only a single VLAN is used in the network or when every VLAN exists on every tagged inter-switch link and simplicity is a major design goal.

PER VLAN Spanning Tree Protocol Option

Per-VLAN mode is the Default Spanning Tree setting on all three switches. In this mode, the switch runs a separate spanning process for each VLAN. Each logical Spanning Tree has its owns Per-VLAN BPDU's which are tagged with the appropriate VLAN Identifier(s). Under this mode, the switch can participate in as many Spanning Tree Domains as there are VLANs defined on the switch. This conforms to a "virtual" bridging model where the switch runs as if each VLAN is a separate logical bridge (separate Address Forwarding Tables, separate spanning trees, etc.). If spanning tree is not required on all VLANs, you can disable it for individual VLANs on a VLAN by VLAN basis. Also, different root bridges can be configured with different bridge priorities based upon VLAN. This will allow load sharing to occur based upon VLAN. Similarly link costs and priorities can be adjusted on a per-VLAN basis allowing further load sharing per VLAN.

Per VLAN Spanning Tree is the recommended method whenever many VLANs are passed over interswitch links, but not every VLAN reside on every interswitch link. If IEEE 802.1D Spanning Tree mode is used without care under these constraints, VLANs can be split due to blocking on inappropriate links. The only time that Per-VLAN mode may become undesirable is when you have more VLANs to manage than the number of Spanning Tree Domains. The only other constraint is to limit the number of outgoing BPDUs.

It is required that the number of outgoing BPDUs be less than 500/ second on all three switches. This means that if you have 50 VLANs you cannot have more than 20 possible paths back to the root bridge (50 VLANS X 20 LINKS X 0.5 BPDU/sec. = 500), or if you have 100 VLANs you cannot have more that 10 possible paths back to the root bridge. These constraints are not generally exceeded in real networks. If these limits are exceeded, you must use 802.1D Spanning Tree mode.

This method can easily inter-operate with legacy IEEE802.1D Devices. The Legacy Devices become part of the VLAN associated with the VLAN port binding with which they are attached. In other words, if there are 3 P550’s in a network running VLANA and VLANB, and three legacy devices connect up through a port configured in VLAN A, the legacy devices will become part of the VLAN A Spanning Tree. The P550’s will participate in two Spanning Tree domains, one for VLAN A containing three bridges and one for VLAN B containing 6 bridges. The legacy devices need not be VLAN aware.

Dual-Layer Spanning Tree Protocol Option

Dual-Layer spanning tree mode is a variation of per-VLAN spanning tree mode with many of the same features. However, instead of using normal BPDUs, which are clear (free of VLAN tags) on clear links and tagged on tagged links, as is the case with Per-VLAN Spanning Tree mode, dual-layer uses a proprietary BPDU. This proprietary BPDU is sent to a special multicast address and contains information about which VLAN the BPDU is associated with. This has an advantage over per-VLAN spanning trees in that this method can support multiple VLANs over a non-tagging link, or when connecting to a bridge/router.

In this mode, Legacy Bridges remain in separate Spanning Tree domains, yet loops between the layer 3 and Legacy domains cannot form. For example; if there are three P550 switches in a network running VLAN A and VLAN B, and three legacy devices connect up through a port configured in VLAN A, the legacy devices remain in their own Legacy Spanning Tree and NOT join the Multilayer Spanning Tree.

In the previous example, all three switches participate in two Spanning Tree domains:

- Domain for VLAN A containing three bridges
- Domain for VLAN B containing three bridges with the legacy domain remaining separate.

The legacy devices need not be aware of the other spanning tree domains. If a loop forms between the Multilayer domains and the legacy domain, the Proprietary BPDU is seen returning to the Multilayer domain through the Legacy domain and the loop is blocked. The Dual-Layer Spanning Tree method is preferred when inter-operating with large legacy bridge networks. Convergence time is reduced, and management is simplified, by allowing the legacy bridges to remain in their own spanning tree domain

Global Disable

You can globally disable Spanning Tree on all three switches, thus preventing any switch port from participating in Spanning Tree. This is only recommended in a very controlled environment where there is no possibility of a loop being placed in the network.

PORT SETTINGS

You can use the “Bridge Ports” option to adjust link costs and priorities per IEEE802.1D. You can also disable Spanning Tree per-port via this option. If you disable Spanning Tree per port, IEEE802.1D definitions are strictly followed. This means that BPDUs are not sent, incoming BPDUs are not processed, and incoming packets are not forwarded. The port is disabled at Layer 2. You can also set the port to Spanning Tree disable on a port if you do not want that port to “Participate”. The port is then put directly into Forwarding State: meaning BPDUs cannot be sent out the port, incoming BPDUs cannot be processed, and received traffic can still be forwarded.

SPANNING TREE DESIGN

Avaya recommends that you consider the following standard IEEE802.1D Guidelines when you design your network, no matter which Spanning Tree mode you decide to use:

- Assure center switches can be forced to be root bridges. For Per-VLAN Spanning Tree, the function of root bridge can be shared among several center switches
- When using standard timers assure the depth of the tree does not exceed 7 bridges when a default bridge timer is used
- Enable FAST START on all ports that contain IPX and DNS clients.

Extensive Fault Tolerance

All three switches are designed to function as backbone switches. You can install each switch in your network's core without creating a single point of failure.

Extensive fault tolerance features include:

- N+1 power. Power supplies share the power supply load. If one fails, the remaining supplie(s) assume the load automatically and the switch management system warns you of the failure.
- Hot-swappable power supplies, fans, and modules - Each power supply can be changed from the switch front panel, without powering down the switch.
- Redundant switch links (using spanning tree and link aggregation groups).
- Front-loadable cables, modules, power, supplies and fans.
- Redundant switch matrix and switch controller modules (layer 2 only).

Buffer and Queue Management

Buffer and queue management relieves congestion in a network. Adding gigabit speeds to existing networks means that there can be a huge disparity between link speeds. For example, anything more than a 1-percent load on a gigabit link could easily overwhelm a 10 Mb/s Ethernet link.

Each switch employs the following buffer and queue management techniques:

- Configurable active backpressure:
  - Half-duplex ports use active backpressure to jam input ports when their frame buffers are full.
  - Full-duplex links use IEEE 802.3z pause control frames to pause traffic when buffers are full.
- Packed frame buffers for optimal memory utilization. The memory management allows virtually 100% utilization of buffer memory.

- Two CoS priority queues that provide flexible queue management algorithms to meet application requirements.
- Large buffer space:
  - 512KB per gigabit port.
  - 128KB additional for outbound 10/100 ports.
    - Configurable queue depth for each of two prioritized packet queues.
    - Configurable priority threshold.
    - Configurable service ratio tunes queue priority.

Routing Overview

All three switches can be configured as an IP, IPX ,and AppleTalk router with virtual interfaces. Virtual interfaces are mapped to physical ports or VLANs. Layer 3 IP traffic is routed between the virtual interfaces.

Ports become members of VLANs by being assigned or by rules. Multiple VLANs can share a single trunk port. In contrast, multiple physical ports can be associated with a single VLAN. In all cases, traffic that arrives and leaves the same VLAN is *bridged*, not routed.

This section provides the following sections:

- Compatibility with the Layer 2 Switch
- Routing with Layer 2 and Layer 3 Modules

Compatibility with the Layer 2 Switch

Each switch is completely backward compatible with all of the layer 2 media modules that the switch currently supports. Layer 2 traffic is routed by sending that traffic to the layer 3 supervisor module. The supervisor module routes all traffic from layer 2 media modules in software as described in the next section, *“"Routing with Layer 2 and Layer 3 Modules"”* .

*** Note:** Layer 2 traffic that does not require routing is bridged independently of the layer 3 traffic based on the MAC address or VLAN information.

Routing with Layer 2 and Layer 3 Modules

When a switch is configured with a mix of layer 2 and layer 3 modules, IP and IPX routing is performed by the layer 3 media modules or the layer 3 supervisor module using special ASICs present on those modules. These ASICs contain an *address cache* (forwarding table) that can contain a maximum of 20,000 cache entries. The address cache entries consist of packet addressing information and next hop information that enable the switch to effectively route the packets to their destination.

The layer 3 supervisor module also maintains a *master routing table* that is kept in the its memory. The master routing table can contain up to 24,000 entries. This routing table enables the supervisor module to keep track of which entries are in each address cache. As a result, each time a change occurs in the master routing table, the layer 3 supervisor module updates the appropriate address caches. For example, if a unicast route is removed from the master routing table, all matching entries in address caches are also removed.

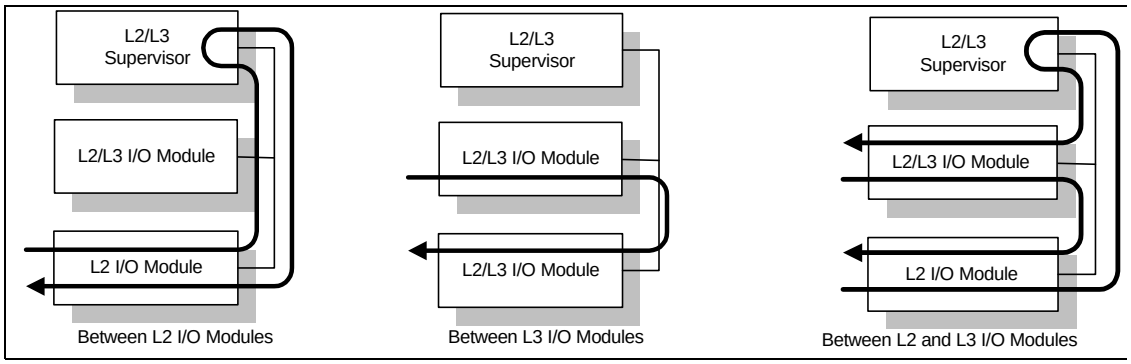
Consequently, when you connect a switch to the network, it begins to receive frames from the network and builds a master routing table (supervisor module) and forwarding tables (address caches of media modules) based on those frames.

This process creates three distinct results:

- All known (learned) layer 3 traffic that requires routing, is routed directly by the layer 3 media module without a need to traverse the switching fabric to get to the supervisor module's software routing function.
- All unknown (not learned) layer 3 traffic must first be sent to the layer 3 supervisor module, where information on the frame is added to the supervisor module's master routing table, then it is added to the address cache of each applicable layer 3 media module.
- Since layer 2 modules have no routing capability, packets that are received by a layer 2 module and the required routing are forwarded by sending the packet to the layer 3 supervisor module. The routing engine on the supervisor module then performs the routing operation for the layer 2 modules and sends the packet back through the switching fabric to the destination port.

Figure 1-5 shows how traffic is routed in a switch.

Figure 1-5. Layer 2 and Layer 3 Routing in a Switch



2 Initialize and Setup of the P550/P880/P882 Switch

Overview

The following information and procedures are provided in this chapter and are common to both layer 2 and layer 3 module configuration:

- Setting Up Your Laptop or PC Monitor
- Configuring the Supervisor Module Using the CLI
- Configuring the Switch Using the Web Agent
- Changing the Console Serial Port Settings
- Configuring Dial-Up Networking
- Managing Configuration Files

*** Note:** The last step in each procedure tells you to click Apply to save any setup or changes you made. This saves the setup or any changes to the **Running config** only. The **Startup config** has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power it off.

To save these changes to the Startup Config, you must copy the **Running config** to the **Startup config**. Refer to the "Copying Configuration Files" section later in this chapter.

Setting Up Your Laptop or PC Monitor

You need a laptop or PC to make a serial line connection to the switch to complete initial switch setup. Table 2-1 lists the settings required for the laptop or PC monitor to communicate with the switch.

Table 2-1. Laptop or PC Monitor Settings

Baud Rate	Stop Bits	Data Bits	Flow Control	Parity
9,600	1	8	Xon/Xoff	None

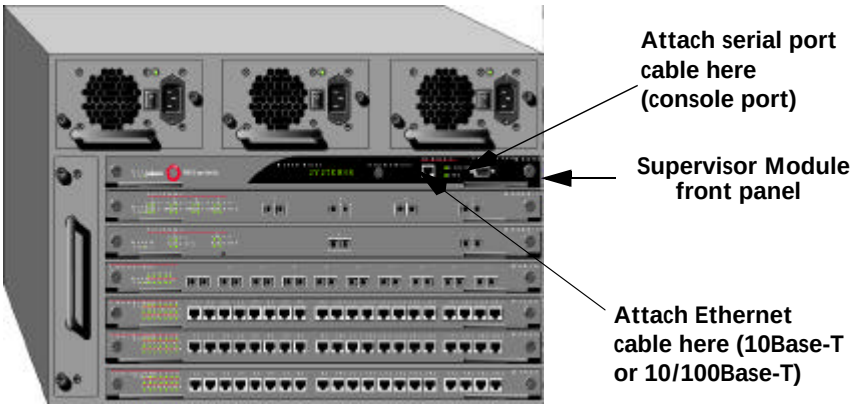
Configuring the Supervisor Module Using the CLI

To connect to the Web Agent, you must first use the serial command line interface (CLI) to configure the switch's IP address and a subnetwork mask on the supervisor module.

To configure the supervisor module using the CLI:

1. Attach a 9-pin straight-through male-to-female serial cable from the serial port on your laptop or PC to the serial port on the supervisor module's front panel (Figure 2-1).

Figure 2-1. Cajun P550 Switch Front View


Attach serial port cable here (console port)
Supervisor Module front panel
Attach Ethernet cable here (10Base-T or 10/100Base-T)

2. Run a terminal emulation program (HyperTerminal, for example) on the attached laptop or PC. Verify that the laptop or PC monitor settings match those listed in Table 2-1.

3. Power up the switch. The switch displays the following startup messages in the terminal emulation program:

```
Booting the operational system, please wait ....

Initializing the file subsystem ... done
Initializing the event subsystem ... done
Initializing the agent subsystem ... done
Initializing the platform ... done
Initializing the switch subsystem ... done

Starting up threads ...
    Periodic Task
    Event
    Network Interface
    Switch Interface
    Telnet Processes
    Ping Process
    Module Manager
    Address Table Aging
    Multicast Pruning
    Front Panel Display
    Download
    Fans Poller
    Power Supplies Poller
    VTP Snooping
    Redundant Controller/Element Poller Task
    Command Line Parser
Powering up modules
Module 1 Powered
Waiting for power cycle to complete (The 17 second power cycle
option)
Module 2 Powered

Initializing the module subsystem ... done

System initialization complete.

Configuring system from Startup Config file [/nvram/
startup.txt] ... done
Boot process complete - system is now operational.(3.0->4.0
conversion)
Creating Startup Config file [/nvram/startup.txt] ... done

Copyright © 1999, All rights reserved by Lucent Technologies
Corporation

This software is furnished under a license and may be used in
accordance with the terms of such license and with the
inclusion of the above copyright notice. This software or any
other copies thereof may not be provided or otherwise made
available to any other person.
No title to and ownership of the software is hereby
transferred.
```

```
Contains software developed by:
Epilogue Technology Corporation
Copyright (c) 1988 - 1996 Epilogue Technology Corporation
TEC Technically Elite Concepts, Inc.,
Copyright (c) 1994 by Technically Elite Concepts, Inc.,
Hermosa Beach, California, U.S.A.

ISI Integrated Systems, Inc.
Copyright 1991 - 1995, Integrated Systems, Inc.

All other trademarks used herein are the property of their
respective owners.

Lucent Technologies Cajun Switch Agent v4.0.0
Press Ctrl-P for previous command, Ctrl-N for next command,?
for help.

Login:
```

*** Note:** Login information and Password prompts are case sensitive.

4. Enter **root** at the **Login** prompt. The password prompt displays.
5. Enter **root** at the **Password** prompt. The command line interface prompt displays. You must now change he command mode to the configure mode so that you can use the `setup` command.
6. Complete the following steps to change the command mode to the configure mode:
   a. Enter the `enable` command.
   b. Enter the `configure` command.
7. Enter the `setup` command. This initiates a series of queries. Answer each query as follows:
   a. Press **Enter** when prompted to change the super user password. This accepts the default of **Yes**
   b. Enter your **old password**. The system then prompts you for a new password.
   c. Enter your **new password**, then re-enter the new password to verify your choice.
   d. Enter the **IP address** for the switch manager's Ethernet console.
   e. Enter the **subnet mask**.
   f. Enter the **default gateway** for the switch.

Figure 2-2 shows the setup command session.

Figure 2-2. Layer 2 and Layer 3 CLI Setup Command Session

```
Welcome to Switch Setup. The brief series of questions
follows will help you to configure this switch. After
completing this process, you will be able to manage the
using:

 - the switch-based HTTP server
 - the Element Management System.

Text in [] is the default answer for each questions.
To accept the default, press ENTER.


Would you like to change the super user password [Yes]?

Old Password: xxxx
New Password: xxxx
Re-type New Password: xxxx
User password changed successfully

What do you want the switch manager's console
Ethernet IP Address to be [0.0.0.0]? 10.0.0.1

What is the subnet mask for your network's
IP address [0.0.0.0]? 255.255.255.0


What is the IP address of the default gateway for this
segment [0.0.0.0]?

You can now connect to the switch using the front-panel
```

Connect one end of a crossover patch cable to the 10Base-T port located on the layer 2 Supervisor module front panel, or the 10/100Base-T port on the layer 3 Supervisor module front panel (Figure 2-1). Connect the other end to an out of band device.

Refer to Table 2-2 for an explanation of the pinouts for the 10Base-t crossover patch cable.

Table 2-2. Pinouts for 10Base-T Crossover Patch Cables

Pin #	Color	Pin #	Color
1	WO	3	WG
2	O	6	G
3	WG	1	WO
4	B	4	B
5	WB	5	WB
6	G	2	O
7	WBr	7	WBr
8	Br	8	Br

Open the web agent after you have completed the out-of-band connection. Refer to the "Opening the Web Agent" section later in this chapter.

Configuring the Switch Using the Web Agent

The switch provides an embedded HTTP server that allows you to set all the switch's parameters from the Web Agent. You can use this interface for quick and simple configuration changes. Refer to Chapter 18, "Analyzing Network Performance Using RMON and Ethernet Statistics" for information on monitoring and configuring the Cajun switch using the Cajun P550 Manager interface.

*** Note:** Although this chapter provides detailed procedures explaining how to configure the switch using the Web Agent, the corresponding CLI commands to do the same task are listed after each procedure. Refer to the *Cajun P550/P880/P882 Command Line Interface Reference Guide* for detailed information about the applicable CLI commands.

Opening the Web Agent

Although the Web Agent supports any frames-capable browser, the system has been specifically qualified with the following browsers:

- Netscape Navigator 4.5 or later
- Microsoft Internet Explorer 3.0 or later

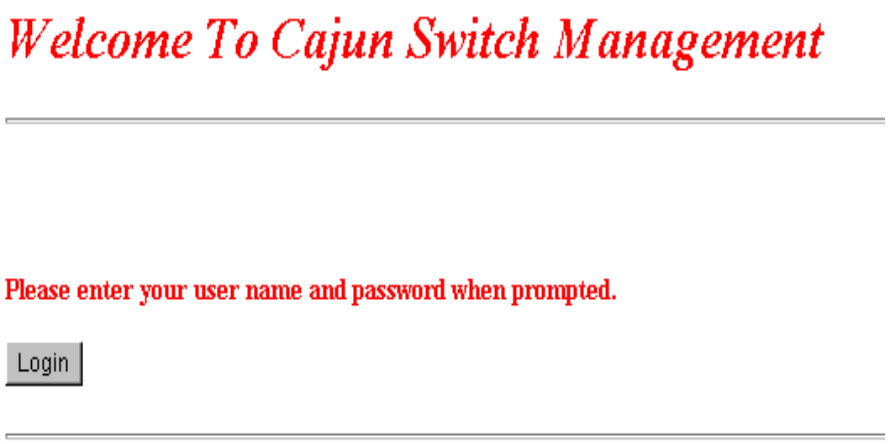
To open to the Web Agent:

1. Start your browser.
2. Enter the URL of the switch you want to manage In the Location field. For example: http://127.255.255.0.

   *** Note:** You must enter a separate IP address for each supervisor module interface (console or inband). For layer 3, you can use can any of the router interfaces.

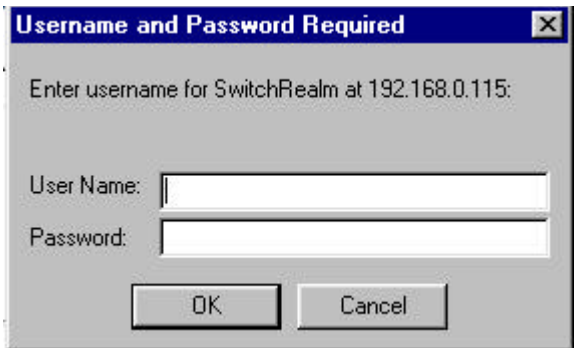
3. Press Enter. The Welcome to Cajun Switch Management window opens (Figure 2-3).

Figure 2-3. Cajun Web Agent Welcome Window



4. Select Login. The Username and Password Required window opens (Figure 2-4).

Figure 2-4. Username and Password Required Window



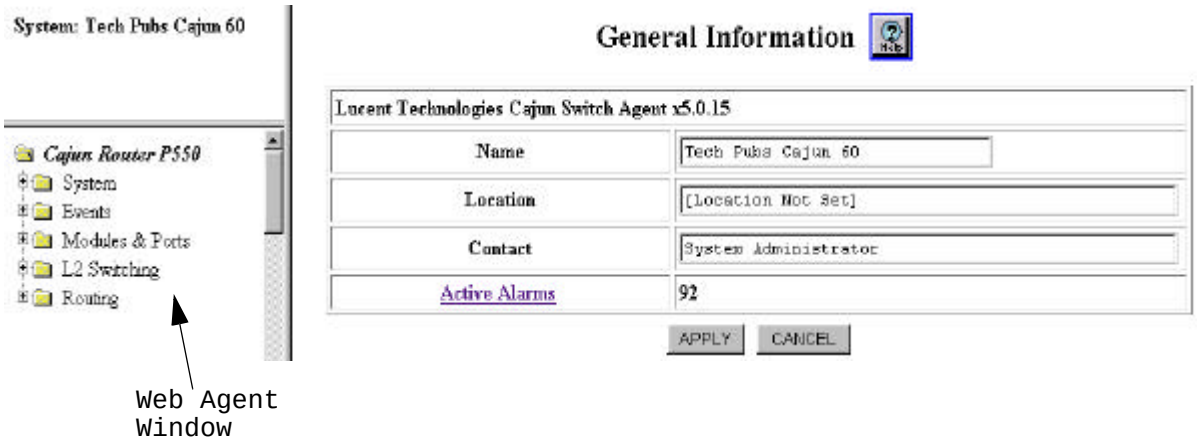
5. Enter a valid user name. The default super user name is root. Press the Tab key to move to the Password field.

6. Enter a valid password. The default password is root.

7. Select OK. The System Information window opens with the Web Agent group folders listed on the left (Figure 2-5).

*** Note:** To optimize security, change the root password for the system as soon as possible.

Figure 2-5. System Information Window

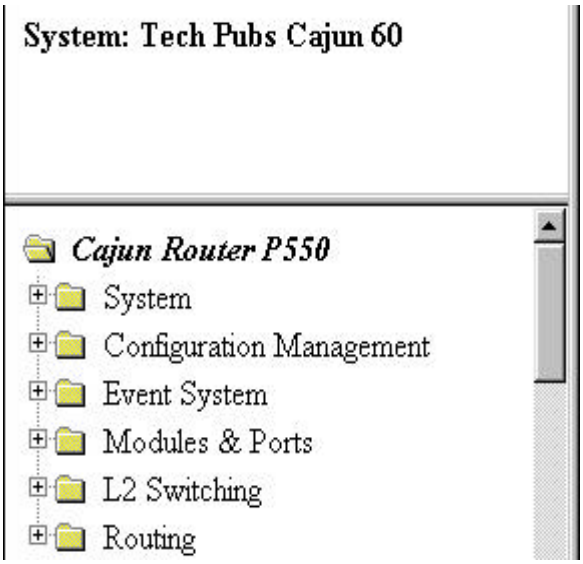


Moving through the Web Agent

To move through the web agent screens:

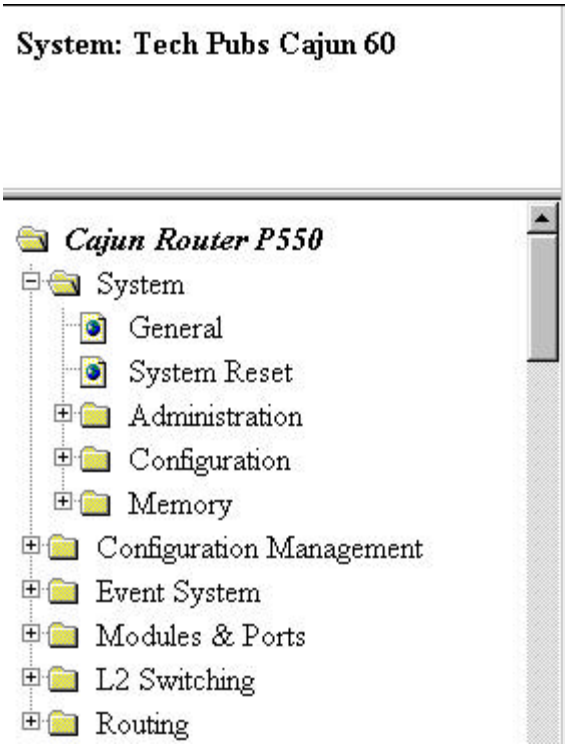
1. Select the plus sign (+) next to the folder that you want to open. That folder opens listing the operations you can perform (Figure 2-6).

Figure 2-6. Opening a Web Agent Folder



2. Select plus sign (+) next to the folder describing the operation you want to perform (i.e., Configuration). The folder opens listing the operations that you can perform (Figure 2-7).

Figure 2-7. Operation Folder Contents



3. Select an operation (i.e., General). The web agent dialog box for that operation opens on the right side.

4. Complete the operation.

The following configuration procedures are written assuming you have already logged onto the Cajun Switch Web Agent.

Setting Up User Accounts

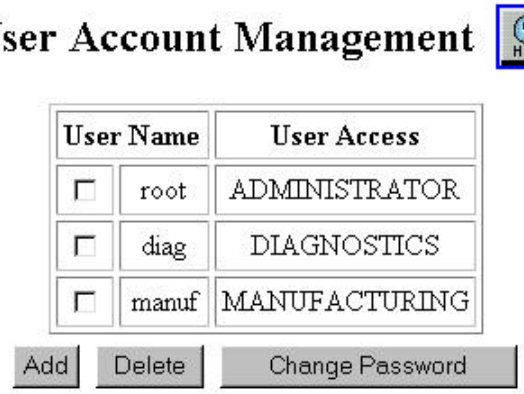
You can setup **User Accounts** using either the web agent or the CLI.

Setting Up User Accounts Using the Web Agent

To setup a user account using the Web Agent:

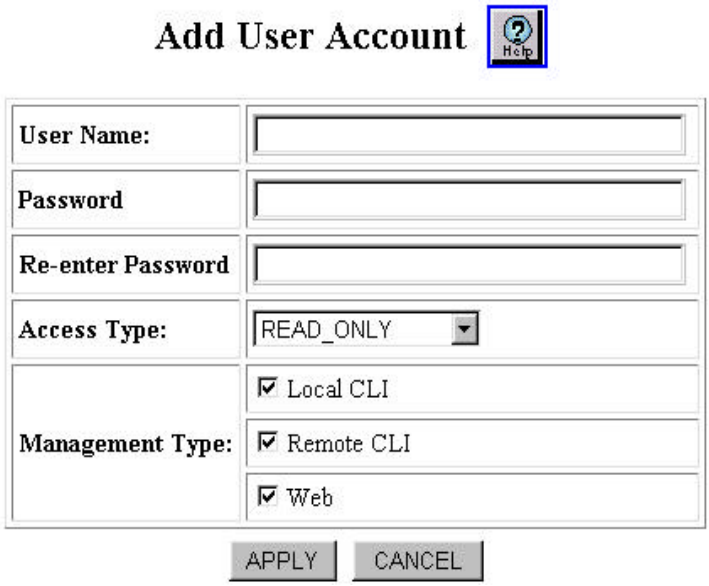
1. Select User Logins from the System > Administration group on the web agent window. The User Account Management dialog box opens (Figure 2-8).

Figure 2-8. User Account Management Dialog Box



2. Select Add. The Add User Account dialog box opens (Figure 2-9).

Figure 2-9. Add User Account Dialog Box.



3. Enter a user name in the User Name field.
4. Enter a password in the Password field.
5. Select an Access Type from the Access Type field pull-down menu. The options are:

- READ_ONLY
- READ_WRITE
- ADMINISTRATOR

Setting Up User Accounts Using the CLI

To setup a user account using the CLI, enter the following command in User mode:

```
> username <name> password [encrypted-type1] <passwd>
[access-type {read-only|read-write|admin}]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Setting Up SNMP Communities

SNMP is identified on a switch through SNMP communities. SNMP communities are configured to manage the switch. You set up SNMP communities using either the web agent or the CLI.

*** Note:** SNMP Version 2c is supported.

All three switches support a maximum of ten SNMP community strings.

Setting Up SNMP Communities Using the Web Agent

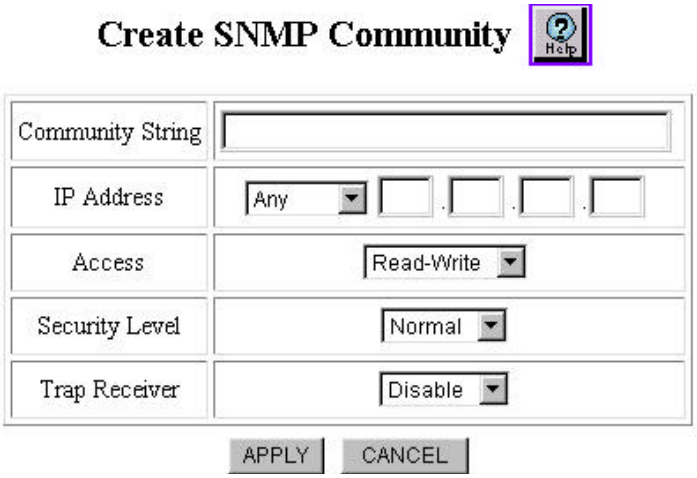
To set the SNMP communities parameters using the web agent:

1. Select SNMP Administration from the System > Administration group on the web agent. The SNMP Community Management window opens (Figure 2-10).

Figure 2-10. SNMP Community Management Window

2. Select CREATE. The Create SNMP Community dialog box opens (Figure 2-11).

Figure 2-11. Create SNMP Community Dialog Box



3. Enter a name for the SNMP community in the Community String field.

4. Select an option from the IP Address field pull-down menu. The options are:

   - Any – for any IP address
   - Specific – Enter an IP Address.

   *** Note:** You cannot enable the trap receiver if you select Any.

5. Select an Access level for this community from the Access field pull-down menu. Refer to Table 2-3 for the Access level field options.

Table 2-3. Access Level Field Options

Access Level	Manager Can...	Manager Cannot...
Read-Only	View switch configuration settings and statistics.	View community strings. Change switch configurations.
Read-Write	View and set switch configuration settings, and view statistics.	View community strings.

Table 2-3. Access Level Field Options continued

Access Level	Manager Can...	Manager Cannot...
Read-Write with Security Level Set to admin	View and set all switch parameters, including community table.	N/A
None	Disable a string without deleting it.	Access any switch features.

6. Select a security level from the Security Level pull-down menu (refer to Table 2-4).

Table 2-4. Security Level Field Options

Option	Allows Access to...
normal	All switch configuration and reporting functions.
admin	All switch configuration and reporting functions, including access to **community configuration**.

7. Select Enable from the Trap Receiver field pull-down menu. Disable is the default

   *** Note:** Select Enable only if you selected Specific from the IP Address field.

8. Click APPLY to save your changes, or CANCEL to clear your selection.

   *** Note:** If you click Apply, the changes are saved in the Running config only. The Startup config has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power it off.

   To save these changes, you must copy the Running config as the Startup configuration. Refer to the section “Copying Configuration Files" section later in this chapter.

Setting Up SNMP Communities Using the CLI

To set the SNMP communities parameters using the CLI, enter the following command:

```
> snmp-server community <string>{ro|rw |none}[{normal| admin}]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Changing the Console Serial Port Settings

You can change the communications settings for the serial port connection on the front panel of the layer 3 supervisor module from the web agent. The switch's console port is initially configured as a TTY Console to support a TTY connection. The layer 2 and layer 3 supervisor modules allow you to reconfigure the console serial port as a PPP Console to support a dial-in PPP connection using a modem.

*** Note:** If you reconfigure the serial port as a PPP console, you can only change the switch's baud rate and flow control parameters. The flow control parameters are limited to None or Xon/Xoff.

Configuring the Serial Console Port as a TTY Console

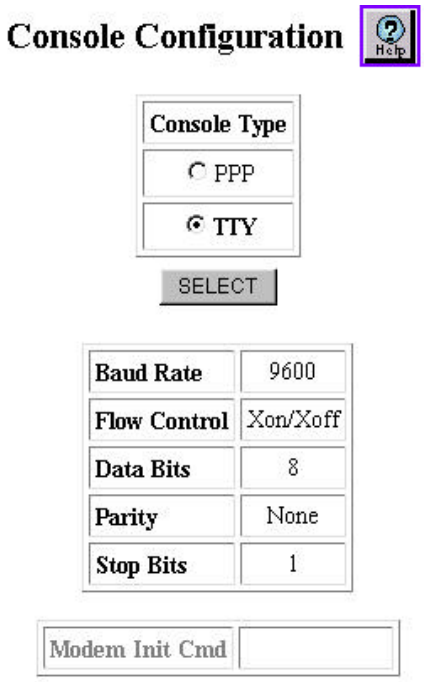
You can configure the serial port as a TTY console using either the web agent or the CLI.

Configuring the Serial Console Port as a TTY Console Using the Web Agent

To configure the console serial port as a TTY Console using the web agent:

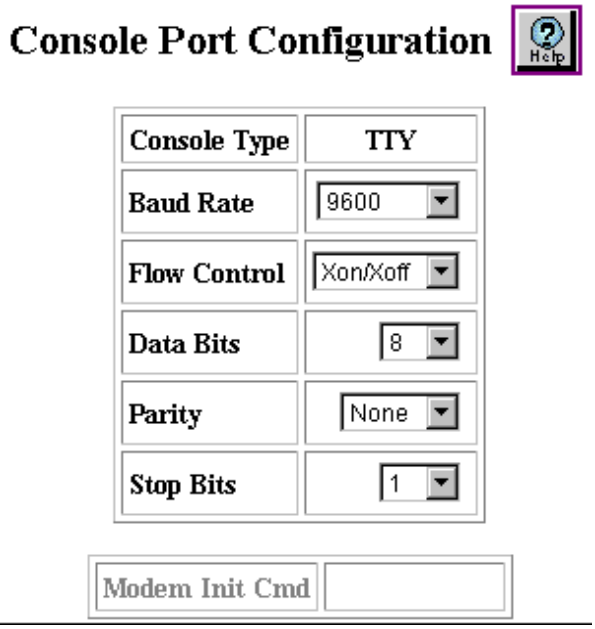
1. Select Console Configuration from the System> Configuration group on the Web Agent. The Console Configuration window opens (Figure 2-12).

Figure 2-12. Console Configuration Window



2. Select TTY as the console type and click SELECT. The Console Port Configuration window opens with TTY displayed in the Console Type field (Figure 2-13).

Figure 2-13. Console Port Configuration Window.



3. Refer to Table 2-5 and configure the other Console Port Configuration dialog box parameters:

Table 2-5. Console Port Configuration Dialog Box Parameters

Option	Default	Available Settings
Baud Rate	9600	300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Flow Control	Xon/Xoff (TTY)	None, Xon/Xoff (TTY)
Data Bits	8	7 or 8
Parity	None	Odd, Even, or None
Stop Bits	1	1 or 2

4. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

Configuring the Serial Console Port as a TTY Console Using the CLI

To configure the console serial port as a TTY Console using the CLI, enter the following command:

```
set console type {tty|ppp}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring the Serial Console Port as a PPP Console

You can reconfigure the serial port as a PPP console to support a dial-in PPP connection using either the web agent or the CLI. Before you can do so, however, you must connect a modem to the switch.

*** Note:** If you do not configure an IP address for the PPP serial interface, the switch immediately sends the modem configuration string. If you type TTY, you will re-access the CLI login prompt.

Connecting a Modem

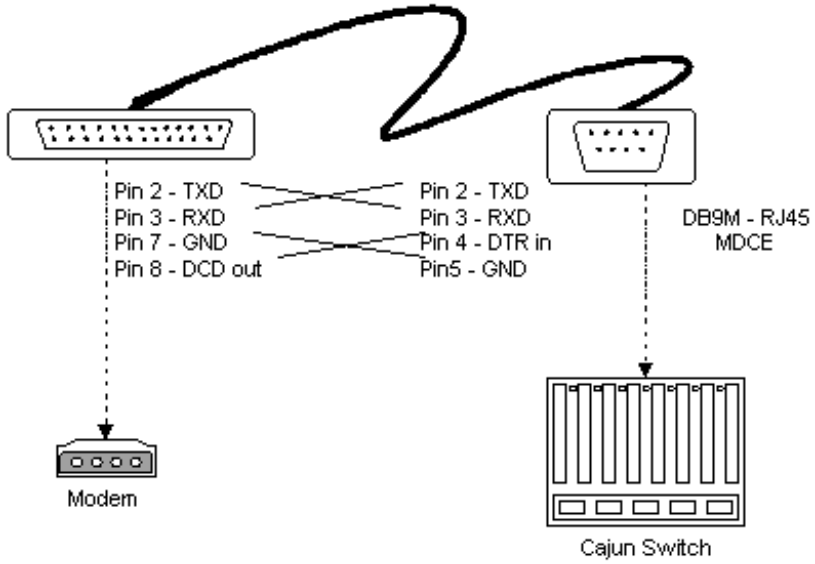
After you connect a modem to your switch with the specified serial cable and connectors, and configure the serial port in PPP mode, the switch will convert the normal Distributed Computing Environment (DCE) interface to a Data Terminal Equipment (DTE) interface that is used by modems.

It then periodically sends the modem configuration string from the serial console port. This synchronizes the baud rates between the modem and the console port and configures the modem to operate with the switch's DTE interface.

To connect a modem (Figure 2-14):

1. Attach a DB25M-RJ45 (P/N 38210003) connector to the modem.
2. Attach the DB9M-RJ45 MDCE connector to the switch's serial console port on the front panel of the switch.

Figure 2-14. Typical Modem Connection to a Switch

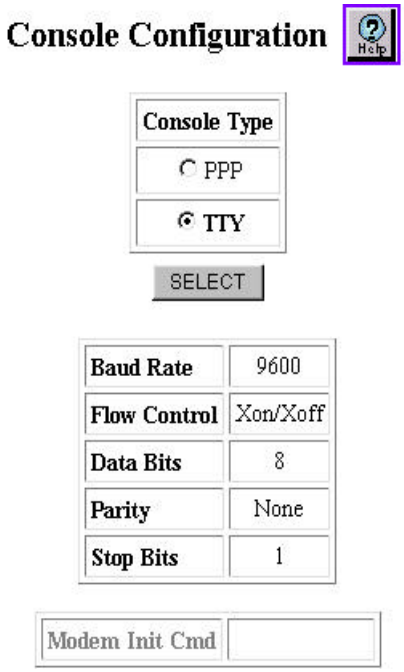


Configuring the Serial Console Port as a PPP Console from the Web Agent

To configure the console serial port as a PPP console from the Web Agent:

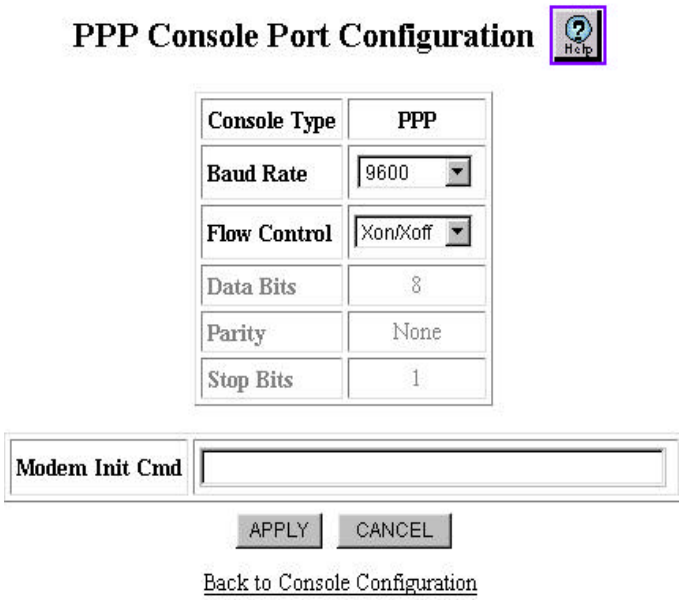
1. Select Console Configuration from the System > Configuration group on the web agent. The Console Configuration dialog box opens (Figure 2-15).

Figure 2-15. Console Configuration Window



2. Select PPP as the console type and click SELECT. The Console Port Configuration window opens with PPY displayed as the Console Type (Figure 2-16).

Figure 2-16. PPP Console Configuration Window.



3. Select a baud rate from the Baud Rate field pull-down menu different from the one already selected.

4. Select an option from the Flow Control field pull-down menu. The options are: None and Xon/Xoff.

   *** Note:** You can only change the baud rate and flow control parameters after you configure the serial port as a PPP console.

5. Enter the modem initialization command in the Modem Init Cmd field. The default modem configuration init command is AT&D0SO=1.

   Refer to Table 2-6 for a definition of the Modem Configuration Init command parameters.

Table 2-6. Modem Configuration String Parameters

Parameter	Definition
&D0	Disable DTR
S0=1	Auto-answer mode (one ring)
CD follows carrier	Depends on modem
E0	Disable local echo
Software Flow Control (Receive and Transmit)	Depends on modem

*** Note:** If you misconfigure the PPP serial console port, you can regain CLI access to correct the configuration parameters. For more information, refer to the "Configuring the Serial Console Port as a PPP Console Using the CLI" section later in this chapter.

Safety Tip: To successfully dial-in with PPP to the switch, you must also configure an IP address and interface for the PPP Serial Interface (Serial-Console). Refer to "Managing Configuration Files", later in this chapter for more information.

6. Click APPLY to save your changes, or CANCEL to clear your selection.

   *** Note:** If you click Apply, the changes are saved in the Running config only. The Startup config has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power it off.

   To save these changes, you must copy the Running config as the Startup configuration. Refer to the "Copying Configuration Files" section in Chapter 2, *Initialize and Setup of the P550/P880/P882 Switch*.

Configuring the Serial Console Port as a PPP Console Using the CLI

To configure the console serial port as a TTY Console using the CLI after you install a mode, enter the following command in Configure mode:

```
>(configure)# set console type {tty|ppp}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Regaining Configuration Access to the PPP Serial Port Console

If you incorrectly configure the PPP serial port console, you cannot regain configuration access to the web agent or the CLI. This is a temporary situation and can corrected.

To regain configuration access to the Web Agent or the CLI when the console port is in PPP mode:

1. Enter `TTY` in the console window. The CLI login prompt displays. It may be necessary to press Enter several times to see the login prompt. You may see the modem init command string.
2. Enter your user name at the Login prompt. The password prompt displays.
3. Enter your password at the Password prompt. The Cajun CLI prompt displays.
4. Enter the PPP configuration commands necessary to start PPP. Refer to the *Cajun™ P550/P220 Command Line Interface Reference Guide* for information about the PPP configuration commands.
5. Enter `exit` at the CLI prompt after you complete your configuration settings to reinvoke the modem control software and exit CLI mode.

   *** Note:** You do not need to exit from CLI if the serial port console has been configured as a TTY console, or if you do not intend to re-attempt connecting using PPP.

Configuring Dial-Up Networking

To configure your PC for dial-up networking with a PPP serial port console:

1. Open My Computer on your PC.
2. Double-click Dial-Up Networking. The Dial-Up Networking window opens.

   *** Note:** You must have dial-up networking installed on your PC.

3. Double-click Make New Connection to configure your modem. The Make New Connection wizard opens.

4. Enter a connection name for the computer you are dialing in the Type a name for the computer you are dialing field.

5. Open the Select a Modem pull-down menu.

6. Select your modem and select Configure. The Modem Properties window opens.

7. Select the Connection tab. The Connection window opens.

8. Select the following from the Connection preferences window:

— Open the Data bits pull-down menu and select 8.

— Open the Parity pull-down menu and select None.

— Open the Stop bits pull-down menu and select 1.

9. Select Advanced. The Advanced Connection Settings window opens.

10. Select Software (XON/XOFF) from the Use flow control field.

11. Select OK to close the window. The Modem Properties window re-opens.

12. Select the Options tab. The Options window opens.

13. Select Bring up terminal window after dialing from the Connection control field and select OK. The Modem Properties window closes and the wizard continues.

14. Select Next from the wizard window and enter the telephone number you are calling.

15. Select Next. The wizard reports that you have successfully configured a modem.

16. Select Finish. The wizard closes and the newly configured connection displays in your Dial-Up networking program group.

17. Select your new connection right click the mouse.

18. Select Properties. The Properties window opens.

19. Select the Server Types tab and de-select all advanced options except TCP/IP.

20. Select TCP/IP Settings. The TCP/IP settings window opens.

21. Select Specify an IP Address and enter the IP address fro the serial port interface.

22. Select Server assigned name server addresses.

23. De-select Use IP header compression and Use default gateway on remote network.

24. Select OK to close the TCP/IP window.

25. Select OK to close the New Connections Properties window.

Using Dial-Up Networking with a PPP Serial Port Console

To use TCP/IP applications (Telnet, HTTP, and SNMP) over your PPP serial port interface:

1. Open My Computer on your PC.

2. Double-click Dial-Up Networking. The Dial-Up Networking program group opens.

   *** Note:** You must have dial-up networking installed on your PC.

3. Double-click the PPP modem you previously created. The Connect To window opens.

4. Enter your password and select Connect. A Pre-Dial Terminal Screen opens.

   When the modem has successfully connected, a Post-Dial Terminal Screen opens.

5. Login in the Post-Dial Terminal screen using your CLI user name and password. It may be necessary to enter several carriage returns to view the Login prompt.

6. At the CLI prompt, go to configuration mode.

7. Enter `set console transfer PPP`. ASCII characters display below the CLI prompt. This is typical while the switch attempts to connect via PPP.

8. Select Continue (F7) from the Post-Dial Terminal screen. PPP verification completes and the Connected To window displays a message that the modem connection has been successfully established.

Managing Configuration Files

You can manage the files that contain the configuration data for your Cajun switch from either the web agent or the CLI. When you first install the switch, or upgrade from a previous installation, your configuration parameters are stored in a **startup.txt** file located in the switch's Non-Volatile Random Access Memory (NVRAM). When the switch is restarted, the startup.txt file runs and stores configuration parameters in volatile RAM as a running configuration.

Any changes you make to the switch configuration are automatically recorded in RAM, but not in NVRAM. When you want to retain your current configuration, you must manually save it to NVRAM through the web agent or the CLI.

For information about how to save your running configuration file to your startup configuration, refer to the "Copying the Running Configuration to the Startup Configuration Using the Web Agent", section later in this chapter. Always view and compare your running and startup configuration files to determine changes that you made to your running configuration.

Viewing Your Running Configuration

To view your running configuration:

- Select Running Config from the Configuration Management group on the web agent window. The Running Configuration displays

  Or

- Enter `show running-config` in priv.mode from the CLI.

Viewing Your Startup Configuration

To view your startup configuration:

- Select Startup Config from the Configuration Management group on the web agent window. The Startup Configuration displays

  Or

- Enter `show startup-config` in priv.mode from the CLI.

Viewing Your Script Execution Log File

Each time the startup.txt file or other script runs, a log file is generated. Log files contain the data returned from the script. You can view log file data from the Script Execution Log File using either the web agent or the CLI.

Viewing Your Script Execution Log File Using the Web Agent

To view your Script Execution Log File from the web agent, select Script Log File from the Configuration Management group on the web agent window. The Script Execution Log file displays

Viewing Your Script Execution Log File Using the CLI

To view your Script Execution Log File from the CLI, enter the following command in priv.mode:

```
> show file_name logfile.txt
```

Copying Configuration Files

If you make any changes, you must save the running configuration as the startup configuration to save the changes. Before you do this, always copy your startup configuration to a file on the switch or on a TFTP server.

You can save the running configuration to the startup configuration and copy the startup configuration to a file using either the web agent or the CLI.

*** Note:** Configuration files are automatically saved as text files using the *.txt extension on your switch.

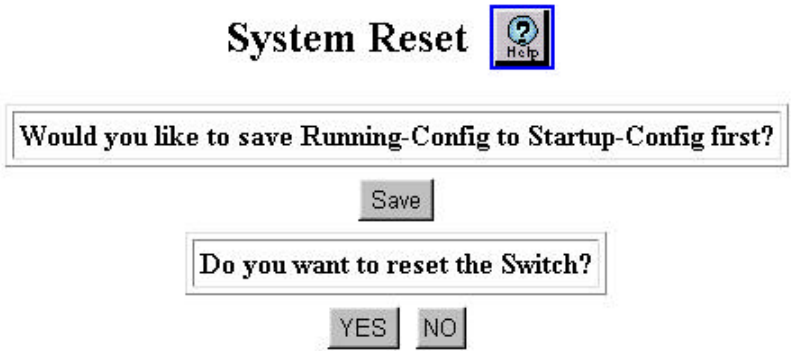
If yo save to a TFTP server, you can edit the startup.txt file using a text editor of your choice and save copies of it with a **.txt** extension.

Copying the Running Configuration to the Startup Configuration Using the Web Agent

To save your running configuration as your startup configuration in NVRAM using the web agent:

1. Select the Config File Management from the Configuration Management group on the e web agent window. The Configuration File Management dialog box opens (Figure 2-17.

Figure 2-17. System Reset Dialog Box



2. Click Save. The running configuration is saved as the startup configuration.

*** Note:** You can also save the running configuration to the startup configuration through the Configuration File Management dialog box. Refer to the "Copying Files" section for that procedure.

Copying the Running Configuration to the Startup Configuration Using the CLI

To save your running configuration as your startup configuration in NVRAM using the CLI, enter the following command in Priv mode:

```
> # copy running-config startup-config
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Copying Files

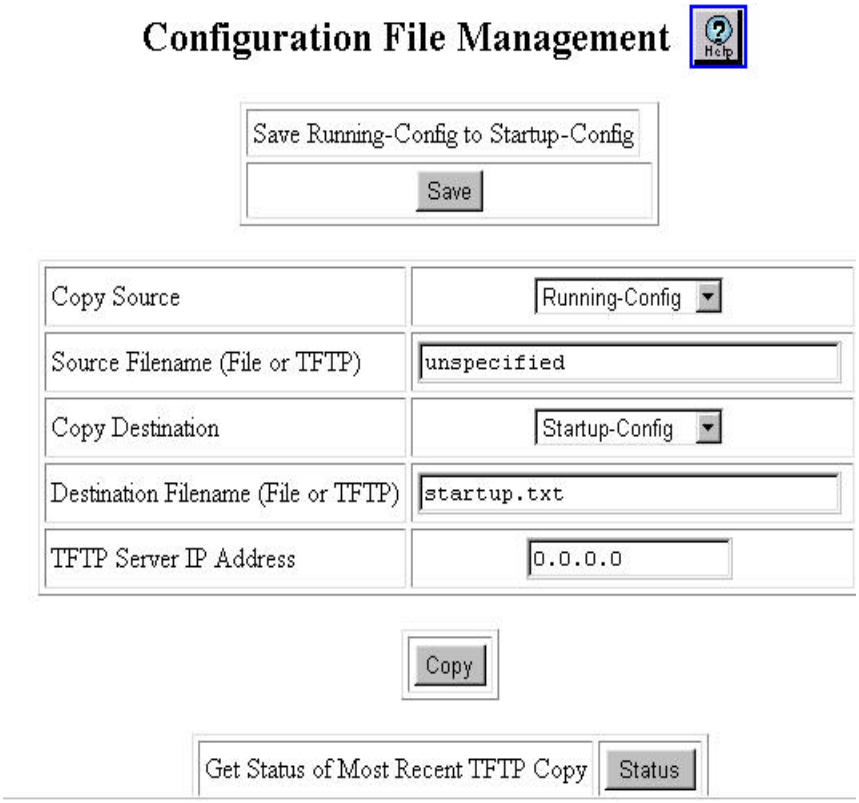
You can copy files to and from multiple locations. For example, if you modify the running configuration and you want to reinstate your startup configuration parameters, you can copy your startup configuration to your running configuration in volatile RAM. You can also upload or download configuration files by copying files from a TFTP server directory to the switch or to a startup or running configuration file. You can copy files using either the web agent or the CLI.

Copy Files Using the Web Agent

To copy files using the web agent:

1. Select File Management from the System > Configuration > Configuration Files group on the web agent window. The Configuration File Management dialog box opens (Figure 2-18).

Figure 2-18. Configuration File Management Dialog Box



2. Refer to Table 2-7 for an explanation of the Configuration File Management dialog box parameters.

Table 2-7. Configuration File Management Dialog Box Parameters

Parameter	Description	Options
Save Running-Config to Startup-Config	Saves the running configuration to the startup configuration	N/A
Copy Source	Specifies the source file to be copied	• **Unspecified** - Specifies an initialized value. • **File** - Specifies a source file located on the switch in NVRAM. • **Running-Config** - Specifies a running configuration. • **Startup-Config** - Specifies a startup configuration. • **TFTP Server** - Specifies a source file located in a directory on a TFTP server.

Table 2-7. Configuration File Management Dialog Box Parameters continued

Parameter	Description	Options
Source Filename	Specifies the path and name of the source file	Source files can be ASCII files in NVRAM available for upload or files located on a TFTP server available for download
Copy Destination	Specifies the location of the destination	• Unspecified- Specifies an initialized value. • **File** - Specifies that a source is copied or downloaded to NVRAM. • **Running-Config** - Specifies that a source is copied to the running configuration. • **Startup-Config** - Specifies that a source is copied to the startup configuration. • **TFTP Server** - Specifies that a source is copied to a TFTP server location.
Destination Filename	Specifies the path and name of the destination file	Configuration files and other files can be copied to NVRAM on the switch or to a TFTP server as a destination location.
TFTP Server IP Address	Specifies the IP address of a source or destination TFTP server	Copy (download) source files, located on a TFTP server, to your running configuration, your startup configuration, or a location on the switch. Or, copy (upload) your configuration files, or a file located on the switch, to a TFTP server.

— File — To copy a file stored on the switch to your running or startup configuration, to a location on the switch, or to a location on a TFTP server.

— TFTP Server — To copy a file stored on a TFTP server to your running or startup configuration or to a file on the switch.

*** Note:** If you select File or TFTP Server, you must also provide the path and filename of the source file in the Destination Filename field.

3. Select one of the following from the Copy Destination pull-down menu.

   — **Running-Config** — Copies your startup configuration, or other file located on the switch or on a TFTP server, to your running configuration.

   — **Startup-Config** — Copies your running configuration, or other file located on the switch or on a TFTP server, to your startup configuration.

   — **File** — Copies your startup or running configuration, another file located on the switch, or a file located on a TFTP server to a file on the switch.

   — **TFTP Server** — Copies your startup or running configuration, or another file located on the switch, to a location on a TFTP server.

   *** Note:** If you select File or TFTP Server, you must also provide the path and filename of the destination file in the Source Destination field.

4. Enter the IP address of the source or destination TFTP server in the TFTP Server IP Address field, if applicable.

5. Click Copy. The source configuration or file is copied to your specified destination.

   *** Note:** The Web Agent returns an `Invalid operation!` error message if you attempt to copy one of the following:

   - The current running configuration to the running configuration.
   - The startup configuration to the same startup configuration.
   - The specified TFTP server to a TFTP server.

Copying Files Using the CLI

To copy files using the CLI, enter the following command in Priv mode**:**

```
># copy running-config +
```

*** Note:** Entering a "+" sign lists all of the applicable options for the `copy running-config` command

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Viewing the Status of a TFTP Transfer

After you have copied the startup configuration or other files to a TFTP server, you can use either the web agent or the CLI to check the status of the TFTP transfer to ensure that files copied correctly.

Viewing the Status of a TFTP Transfer Using the Web Agent

To view the status of a TFTP transfer using the web agent:

1. Select File Management from the System > Configuration > Configuration Files group on the web agent window. The Configuration File Management dialog box opens (Figure 2-18).
2. Select Status from the Get Status of Most Recent TFTP Copy field. A status message displays in the Config File Mgmt Status window.

Viewing the Status of a TFTP Transfer Using the CLI

When you do a transfer using the CLI, the status of the TFTP transfer is immediately returned.

*** Note:** > You cannot view the status of a TFTP transfer done using the CLI from the Get Status of Most Recent TFTP Copy field on the web agent.

3 Configuring System Information

Overview

The following information and procedures are provided in this chapter and are common to both layer 2 and layer 3 module configuration:

- Setting Up Your Laptop or PC Monitor
- Configuring the Supervisor Module Using the CLI
- Configuring the Switch Using the Web Agent

Managing System Information

You can manage system information from either the web agent or the CLI. The following procedures to manage your system information are provided in this section:

- Entering General System Information
- Enabling the Simple Network Time Protocol (SNTP)
- Setting Summer Time Hours
- Displaying the Power System Statistics
- Displaying Cooling System Statistics
- Performing a Reset

*** Note:** The last step in each procedure tells you to click Apply to save any setup or changes you made. This saves the setup or any changes to the Running config only. The Startup config has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power it off.

To save these changes to the Startup Config, you must copy the Running config to the Startup config. Refer to the "Copying Configuration Files," in Chapter 2, *"Initialize and Setup of the P550/P880/P882 Switch"*.

Entering General System Information

You can enter general information about your system using either the web agent or the CLI.

Entering General System Information Using the Web Agent

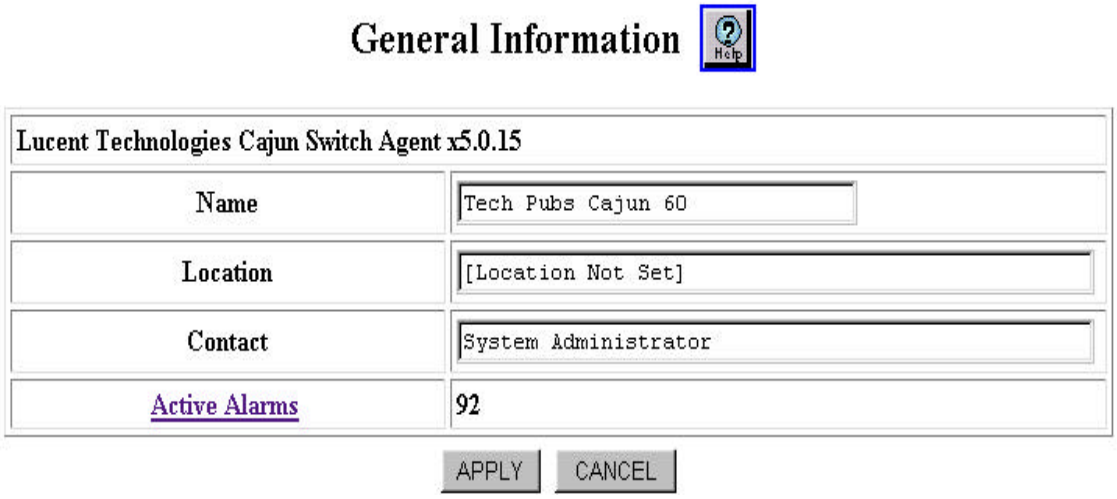
You can enter general system information using the following Web Agent fields:

- Switch name
- Device location
- Device contact

To enter general system information from the web agent:

1. Select General Information from the System group on the web agent window. The General Information dialog box opens (Figure 3-1).

Figure 3-1. System Information Window



2. Enter the switch name in the Name field.
3. Enter the location for the switch (for example, floor, closet in the Location field.
4. Enter the person who should be contacted in the event of a problem in the Contact field.
5. Click APPLY to save your changes, or CANCEL to clear your selection.

Enabling the Simple Network Time Protocol (SNTP)

You can enable SNTP on your switch using either the web agent or the CLI. Enabling SNTP automatically synchronizes time on all computers, switches, and other devices connected to your switch.

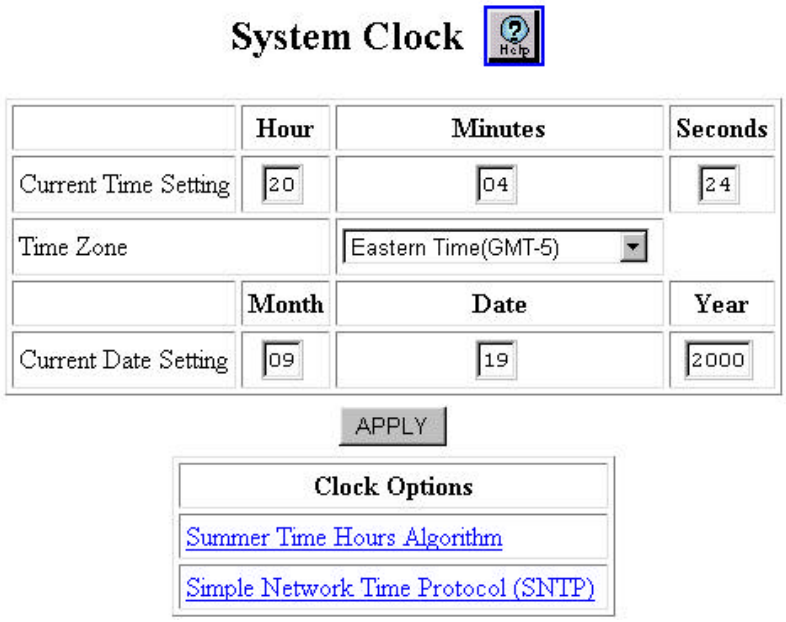
When you enable SNTP, you are required to set your time zone and the rule or dates of Summer Time Hours for your location. For information about setting one-time summer hours, refer to "Setting One-Time Summer Time Hours" later in this chapter. For information about setting Summer Time Hours, refer to "Setting Summer Time Hours" later in this chapter.

Enabling SNTP Using the Web Agent

To enable SNTP on your switch using the web agent:

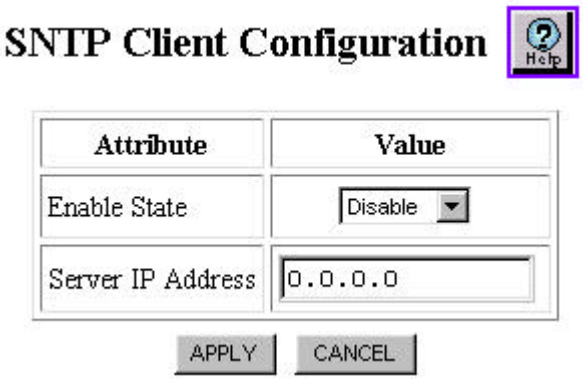
1. Select System Clock from the System > Configuration group on the web agent window. The System Clock dialog box opens (Figure 3-2):

Figure 3-2. System Clock Dialog Box.



2. Select Simple Network Time Protocol (SNTP) from the Clock Options box. The SNTP Client Configuration window opens (Figure 3-3).

Figure 3-3. SNTP Client Configuration Dialog Box



3. Select Enable from the Enable State pull-down menu. The default is Disable.
4. Enter the server IP address in the Server IP address field for the switch on which you want to enable SNTP.
5. Click APPLY to save your changes, or CANCEL to clear your selection.

Enabling SNTP Using the CLI

To enable SNTP on your switch using the CLI, enter the following command in Configure mode:

```
> (configure)# sntp server <ip-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Setting Summer Time Hours

Summer Time Hours, also referred to as Daylight Savings Time (DST), is the strategy of moving clocks ahead to provide greater amounts of daylight in the afternoon and to standardize time with other parts of the world. In many parts of the world, the Summer Time Hours algorithm is based on a standardized rule. For example, in the Western hemisphere, the rule used by most locations in Canada, Mexico, and the United States is to set clocks forward by one hour at 2:00 a.m. on the first Sunday in April and back an hour at 2:00 a.m. on the first Sunday in October annually. Many countries in Europe and Asia follow similar rules. The offset, or amount of time by which the clock is set forward or backward, varies from country to country.

Many parts of the world follow a one-time change of Summer Time Hours. When you configure the switch for these locations, you reset the clock by specifying a scheduled time and date.

This section provides the following procedures:

- Setting Recurring Summer Time Hours
- Setting One-Time Summer Time Hours

*** Note:** If you upgrade your switch from a previous version, the local time settings are saved as Greenwich Mean Time values. Always change the Summer Time Hours Algorithm before you set the clock.

Setting Recurring Summer Time Hours

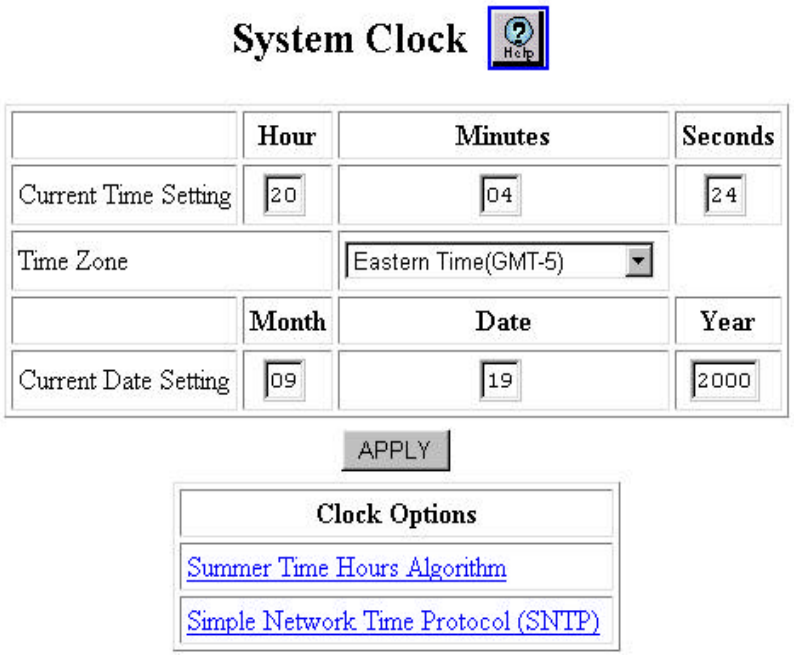
You can set recurring summer time hours using either the web agent or the CLI.

Setting Recurring Summer Time Hours Using the Web Agent

To set recurring Summer Time Hours using the web agent:

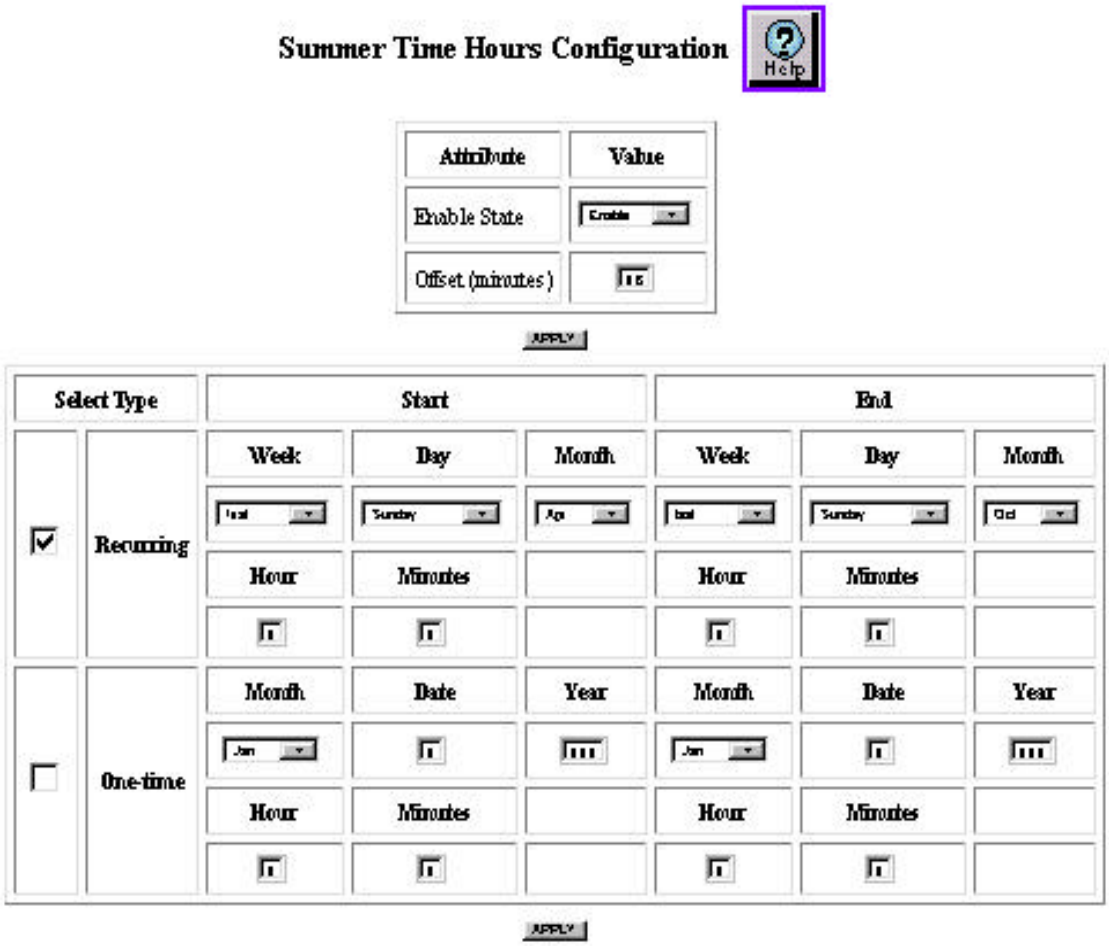
1. Select System Clock from the System> Configuration group on the web agent. The System Clock dialog box opens (Figure 3-4).

Figure 3-4. System Clock Dialog Box



2. Select Summer Time Hours Algorithm from the Clock Options field. The Summer Time Hours Configuration dialog box opens (Figure 3-5).

Figure 3-5. Summer Time Hours Dialog Box



3. Select Enable from the Enable State pull-down menu.

4. Enter the reset value for the clock in minutes in the Offset field. For example, if you intend to reset the clock forward or backward by one hour, keep the default value of 60 minutes.

5. Set the Summer Time Hours that recur annually:

   a. Select the check box in the Recurring field.

   b. Select the values for the Week, Day, and Month when the Summer Time Hours are to start and end.

   c. Enter values for the Hour and Minutes when Summer Time Hours are to start and end.

6. Click APPLY to save your changes, or CANCEL to clear your selection.

Refer to Table 3-1 for detailed information about the fields in the Recurring Summer Time Hours section of the Summer Time Hours Configuration dialog box.

Table 3-1. Recurring Summer Time Hours Parameters

Parameter	Definition
Recurring	Select if Summer Time Hours is defined by a rule such as Daylight Savings Time (DST. All Start and End fields associated with Recurring Summer Time Hours provide the default values for Daylight Savings Time). When you select Recurring Summer Time Hours, you indicate the time, in hours and minutes, on a specified day, week, and month that Summer Time Hours begin and end.
Start	Specifies the start of Summer Time Hours.
End	Specifies the end of Summer Time Hours.
Week	Select the week during which you want recurring Summer Time Hours to start or end. The selected week should reflect the day on which Summer Time Hours start. For example, if Summer Time Hours start on the first Sunday in April, select the First week. Options include: • **First -** First week of the month, the default Start value, when Daylight Savings Time starts in the Western hemisphere. • **Second -** Second week of the month. • **Third -** Third week of the month. • **Fourth -** Fourth week of the month. • **Last -** Remaining days of the month that form the last week of the month. Last is specified as the default End value, denoting when Daylight Savings Time ends in the Western hemisphere.

***Table 3-1. Recurring Summer Time Hours Parameters** continued*

Parameter	Definition
Day	Select the day of the week when you want recurring Summer Time Hours to start or end. Options are based on a seven-day week and include: • **Sunday -** the default Start and End values. In the Western hemisphere, DST starts on the first Sunday in April and ends on the last Sunday in October. • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday
Month	Select the month when recurring Summer Time Hours start or end. The twelve months of the Gregorian calendar are provided. For recurring Summer Time Hours, the default Start value is April, the month during which DST starts in the Western hemisphere. The default End value is October, the month during which DST ends in the Western hemisphere.
Hour	Enter a value to represent the hour when Summer Time Hours start or end for Recurring settings. For Recurring Summer Time Hours, the default value is 02, meaning 2:00 a.m., for both Start and End hours.
Minutes	Enter a value to represent the number of minutes into the hour when Summer Time Hours start or end for Recurring Summer Time Hours. The default value is 00 for both Start and End minutes.

Setting Recurring Summer Time Hours Using the CLI

To set recurring Summer Time Hours using the CLI, enter the following command from Configure mode:

```
> (configure) clock summer-time recurring <week>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Setting One-Time Summer Time Hours

You can set one-time summer time hours using either the web agent or the CLI.

Setting One-Time Summer Time Hours Using the Web Agent

To set Summer Time Hours that are not based on a standard rule using the web agent:

1. Select System Clock from the System> Configuration group on the web agent window. The System Clock dialog box opens (Figure 3-4).
2. Select Summer Time Hours Algorithm from the Clock Options field. The Summer Time Hours Configuration window opens (Figure 3-5).
3. Select Enable from the Enable State pull-down menu. The default is Disable.
4. Enter the reset value for the clock in minutes in the Offset field. For example, if you intend to reset the clock forward or backward by one hour, keep the default value of 60 minutes.
5. Select the check box next to the One-Time field to set the date and time for Summer Time Hours on a one-time basis:
   a. Enter the specific Month, Day, and Year when the Summer Time Hours start and end.
   b. Enter the Hour and Minutes when the Summer Time Hours start and end.
6. Click APPLY to save your changes, or CANCEL to clear your selection.

Refer to Table 3-2 for detailed information about the One-Time field parameters for the Summer Time Hours Configuration dialog box.

Table 3-2. One-Time Summer Time Hours Configuration

Parameter	Definition
One-time	Select if Summer Time Hours change one time, such as on a specified date. When you select one-time Summer Time Hours, you indicate the time and date on which Summer Time Hours begin and end.
Start	Specifies the start of Summer Time Hours.
End	Specifies the end of Summer Time Hours.
Week	Select the week of the month during which you want recurring Summer Time Hours to start or end. Options include: • **First** - First week of the month, the default Start value, when Daylight Savings Time starts in the Western hemisphere. • **Second** - Second week of the month. • **Third** - Third week of the month. • **Fourth** - Fourth week of the month. • **Last** - The final days of a month, such as the 29th, 30th, and 31st days of a month. Last is specified as the default End value, denoting when Daylight Savings Time ends in the Western hemisphere.
Day	Select the day of the week when you want recurring Summer Time Hours to start or end. Options are based on a seven-day week and include: • **Sunday** - The default Start and End values. In the Western hemisphere, DST starts on the first Sunday in April and ends on the last Sunday in October. • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday
Month	Select the month when one-time Summer Time Hours start or end. The twelve months of the Gregorian calendar are provided. For a one-time setting of Summer Time Hours, the default value for start and end months is January.

Table 3-2. One-Time Summer Time Hours Configuration continued

Parameter	Definition
Hour	Enter a value to represent the hour when Summer Time Hours start or end for One-time settings. The default value is 00.
Minutes	Enter a value to represent the number of minutes into the hour when Summer Time Hours start or end for One-time Summer Time Hours. The default value is 00 for both Start and End minutes.

Setting One-Time Summer Time Hours Using the CLI

To set Summer Time Hours that are not based on a standard rule using the CLI, enter the following command from Configure mode:

```
> (configure)# clock summer-time date
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Setting the System Clock

The system clock is used for setting traps, alarms, and other events on the switch.

*** Notes:** You must set SNTP and Summer Time Hours before you can set the system clock. Refer to "Enabling the Simple Network Time Protocol (SNTP)" and "Setting Summer Time Hours" earlier in this chapter.

The system clock does not automatically change with Daylight Savings Time.

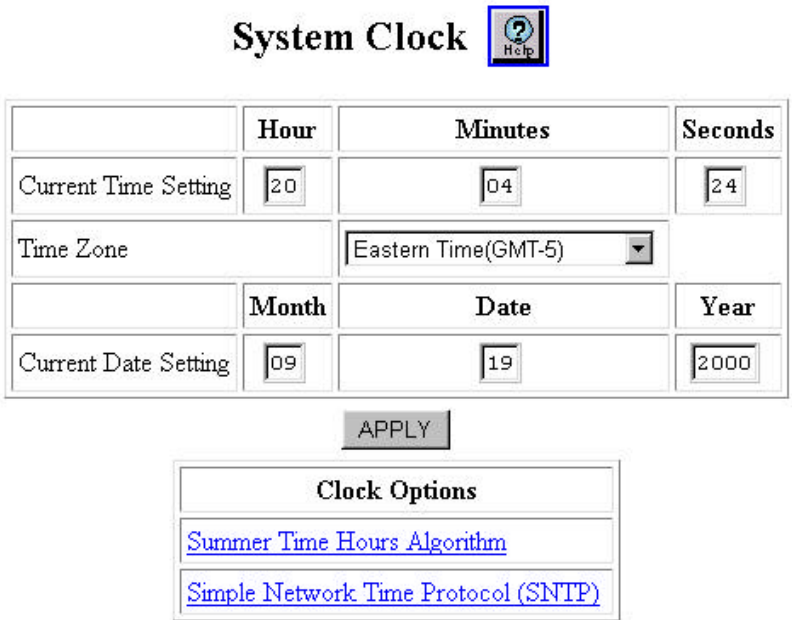
You can set the system clock from either the web agent or the CLI.

Setting the System Clock Using the Web Agent

To set the system clock using the web agent:

1. Select System Clock from the System > Configuration group on the web agent window. The System Clock dialog box opens (Figure 3-6).

Figure 3-6. System Clock Dialog Box



2. Enter the time in the Current Time Setting Hour, Minutes, and Seconds fields using 24-hour time format (for example, 10 p.m. is 22 00 00.
3. Select the time zone for your area from the Time Zone pull-down menu.
4. Enter the current Month, Date, and Year in the Current Date Setting fields.
5. Click APPLY to save your changes, or CANCEL to clear your selection.

Setting the System Clock Using the Web Agent

To set the system clock using the CLI, enter the following command from Priv mode:

```
> clock set <time> <date> <year>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Setting the Temperature System

You can set the upper and lower temperature warning systems for your switch's backplane and slot 1. These warning systems cause the following to happen if the temperatures you set are reached:

- The Supervisor modules shut down the switching modules if the temperature reaches the Shutdown temperature.
- The modules are restarted if the temperature goes below the Upper Warning Temperature.

The default Shutdown temperatures are conservative for the slot 1 sensor (50° C and backplane sensor (50° C. They can be safely set to 60° C, but settings higher than 60° C are not recommended. You can set the shutdown temperature to a value lower than 50° C to ensure prompt notification if a fan fails.

You can set the temperature system using either the web agent or the CLI.

Setting the Temperature System Using the Web Agent

To configure the temperature warning systems using the Web Agent:

1. Select Temperature from the System > Configuration group on the web agent window. The Temperature System dialog box opens with the current temperature settings (Figure 3-7).

Figure 3-7. Temperature System Window

Temperature System Help

	Slot 1 Sensor	Backplane Sensor	CPU Sensor
Shutdown Temperature	50 °C	50 °C	100 °C
Upper Warning Temperature	45 °C	45 °C	85 °C
Current Temperature	**31 °C**	**34 °C**	**44 °C**
Lower Warning Temperature	5 °C	5 °C	5 °C
Low Warning Temperature	0 °C	0 °C	0 °C
DEFAULTS	APPLY	APPLY	APPLY

2. Enter your desired temperature warnings in the slot 1 Sensor, and the Backplane Sensor fields.

   *** Note:** If your switch is a layer 3 switch, you must also enter a temperature warning in the CPU Sensor field.

3. Click APPLY to save your changes, or CANCEL to clear your selection.

Setting the Temperature System Using the CLI

To configure the temperature warning systems using the CLI, enter the following command from Configure mode:

```
cajun>(configure)# set temperature <backplane-
sensor> <cpu-sensor> <probe>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying the Power System Statistics

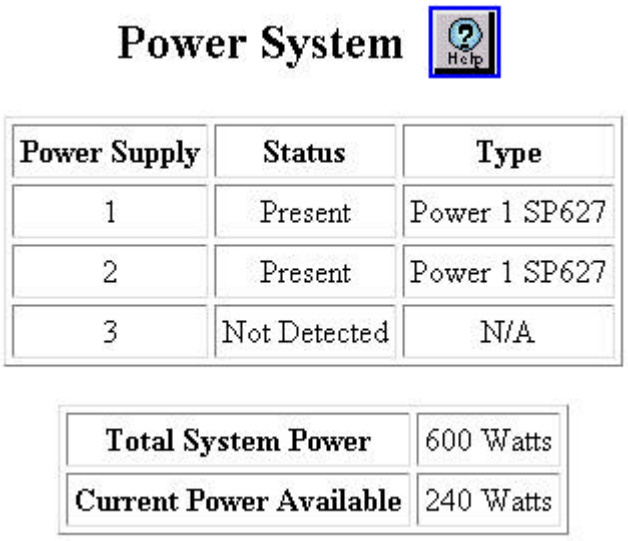
You can display the statistics for your switch's power system from the either the web agent and the CLI.

Displaying the Power System Statistics Using the Web Agent

To display your switch's power system statistics using the Web Agent:

1. Select Power System from the System>Configuration group on the web agent window. The Power System dialog box opens with your switch's current power statistics. (Figure 3-8.

Figure 3-8. Power System Window



2. Refer to Table 3-3 and review the Power System dialog box parameters:

Table 3-3. Power System Dialog Box Parameters

Parameter	Definition
Power Supply	Identifies the power supply
Status	indicates whether the power supply is detected.
Type	Describes the type of power supply detected.
Total System Power	Displays the total system power in Watts.
Current Power Available	Displays the current power available.

*** Note:** You will only see 600W of available power displayed in the Total System Power field even if you have three power supplies installed. The switch only uses power from two of the three power supplies. The third power supply is a redundant power supply and is used only if one of the other power supplies fails.

Displaying the Power System Statistics Using the CLI

To display your switch's power system statistics using the CLI, enter the following command from the Priv mode:

```
> show system power
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying Cooling System Statistics

You can display the statistics for your switch's cooling system from either the web agent or CLI.

Displaying the Cooling System Statistics Using the Web Agent

To display your switch's cooling system statistics using the web agent:

1. Select Cooling System from the System > Configuration group on the web agent window. The Cooling System dialog box opens with your switch's current cooling system status (Figure 3-9).

Figure 3-9. Cooling System Window

2. Check the Status column to ensure that all the individual components are operational.

3. If a component's status is non-operational, power down the switch and contact a service representative to diagnose the failing unit.

Displaying the Cooling System Statistics Using the CLI

To display your switch's power system statistics using the CLI, enter the following command from Priv mode:

```
> show system fans
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Performing a Reset

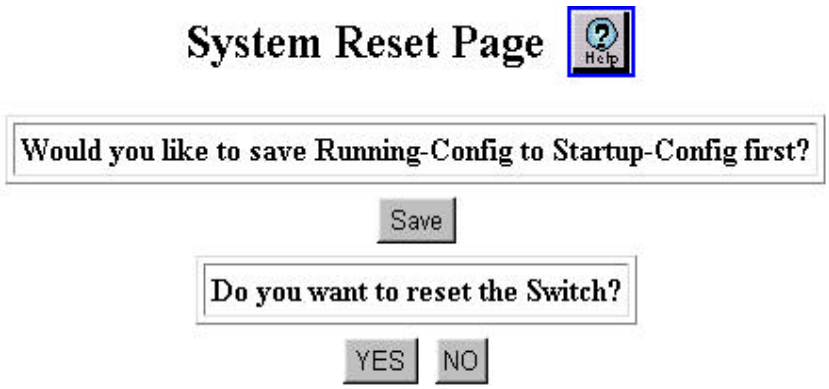
You can reset your switch from either the web agent or the CLI.

Performing a Reset Using the Web Agent

To reset your switch using the web agent:

1. Select System Reset from the System group on the web agent window. The System Reset Page dialog box opens (Figure 3-10).

Figure 3-10. System Reset Page Window



2. Select Save to save your Running Configuration (Running-Config to the startup configuration (Startup-Config before performing a system reset.

   *** Note:** If you do not save your you Running-Config to Startup-Config before you reset the switch, you will lose all of the modifications you made.

3. Click YES to reset the switch, or NO to cancel the operation.

Performing a Reset Using the CLI

To reset your switch using the CLI, enter the following command from Priv mode:

```
> reset
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

4 Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping

Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- VLAN Operation
- Creating and Implementing VLANs
- Using Spanning Tree Setup and Monitoring
- Using Hunt Groups to Aggregate Bandwidth between Switches
- Configuring VLAN Trunk Protocol (VTP) Snooping

VLAN Operation

VLAN operation is based on three sets of rules:

- Ingress Rules
- Forwarding Rules
- Egress Rules

Ingress Rules

Every frame received by the switch is classified to one VLAN. There are two ways in which frames are classified to VLANs:

- Untagged frames are classified to the VLAN associated with the port on which the frame is received (Port-based VLANs).
- Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.

***Note:** The switch supports a feature called Automatic VLAN Creation for tagged frames. When this feature is enabled, the switch creates new VLANs when it receives packets from previously unknown VLANs.

Forwarding Rules

These rules determine the set of ports on the switch through which members of the VLAN can be reached. This is called binding a port to a VLAN. A port may be bound to a VLAN using four methods:

- Setting the Port VLAN attribute in the Switch Port Configuration dialog box of the port form. This identifies the VLAN to which all untagged frames received on the port are forwarded.

  ***Note: Note:** A port has one Port VLAN. Changing this to a new VLAN removes the port from the old VLAN.

- Setting the VLAN Binding attribute in the Switch Port Configuration dialog box to Bind to All. This causes the port to be bound to all VLANs known to the switch (for example, all current VLANs and all VLANs added in the future).
- Setting the VLAN Binding attribute in the Switch Port Configuration dialog box to Bind to Received. This causes the port to be bound to all VLANs (as identified by the VLAN tag in tagged frames) received on this port. Consequently, ports are bound to those VLANs that actually have members that are reachable through the port.
- Manually creating a VLAN Switch Port via the CLI.

Egress Rules

For a given port/VLAN combination, egress rules determine whether frames transmitted from the port on the VLAN are tagged or untagged. This is accomplished by setting the Trunking Mode attribute in the Switch Port Configuration dialog box.

For example, choosing the IEEE 802.1Q trunk mode causes all frames transmitted out of the port to be tagged using the IEEE 802.1Q tag header format. Individual port/VLAN combinations may be changed to cause frames transmitted from the port to be untagged for particular VLANs.

Port-Based VLANs

VLAN assignment of a packet is based on global VLAN ID. Regardless of any name you assign to a VLAN, the switch looks only at the VLAN ID number to determine a packet's VLAN destination.

Creating and Implementing VLANs

Adding users to VLANs includes:

- VLAN Considerations
- Creating a VLAN
- Assigning Ports to VLANs

VLAN Considerations

Be aware of the following issues when configuring VLANs:

- The default setting for Initial Hash Table Size (a number used to determine how much space is initially reserved for new address tables) supports 58 simultaneous VLANs (the switch supports 1,000 VLANs). To increase the number of VLANs you can implement, simply decrease the initial hash table size for each new address table instance.
- If you set a port's VLAN trunking mode to **Clear**, make sure not to change the VLAN Binding Type from the default value: **Static**.

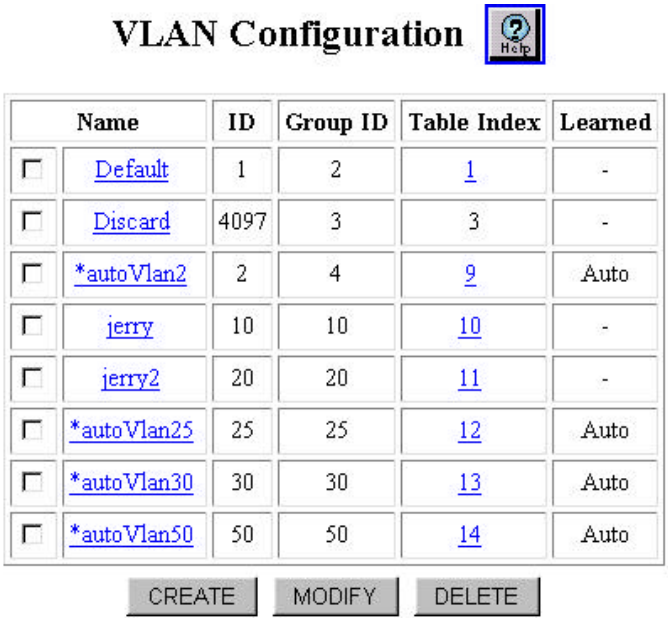
- If you are using both the VLAN auto-learning feature and the Binding Type Bind to Received, make sure that you set the binding type before you set Autolearn to enable or else the port may not be automatically added to the VLAN
- VLAN #4095 is for internal use only and cannot be configured by the user.

Creating a VLAN

To create a VLAN:

1. Select Configuration from the L2 Switching > VLANs group on the Web Agent window. The VLAN Configuration dialog box opens (Figure 4-1).

Figure 4-1. VLAN Configuration Dialog Box



2. Click CREATE. The Create VLAN dialog box opens Figure 4-2).

Figure 4-2. Create VLAN Dialog Box

3. Enter a name for the VLAN in the Name field.

4. Enter an unused VLAN ID (between 1 and 4095) in the ID field. VLAN IDs are global and must be consistent from switch to switch, even when switches are manufactured by different vendors.

5. Refer to Table 4-1 to configure the Create VLAN dialog box parameters:

Table 4-1. Create VLAN Dialog Box Parameters

Parameter	Definition
Name	Name assigned to this VLAN.
ID	Identifier used throughout the network to identify this VLAN. If you want ports on more than one device to participate in a particular VLAN, you must use the same VLAN ID to identify the VLAN on every device.
Initial Hash Table Size	Sets the number of layer 2 address entries used to store information for this VLAN. Use the default value. The general implementation rule is: Use a smaller size when you implement lots of VLANs (more than 50). Use a larger size when you have lots of MAC addresses on the same VLAN in the network (more than 16,000). Note: The number of addresses for a given hash table is approximately 4:1 (for example, if you have a hash table of 16 bytes, the VLAN can hold 64 addresses in it's table instance.
Auto Increment HT Size	Determines whether the number of memory "buckets" used by this VLAN's address table adjusts automatically when memory use become inefficient. Select true if you want the HT size to increase when the number of entries belonging to this VLAN reaches a pre-defined threshold. Select **false** to disable this feature.

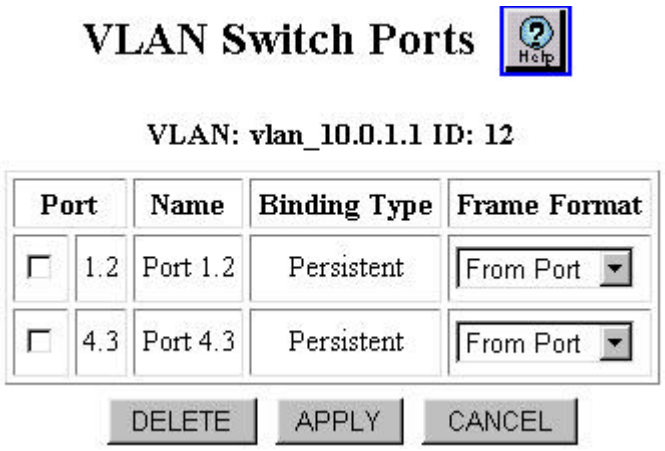
6. Click APPLY to create the new VLAN, or CANCEL to restore previous settings.

Configuring VLAN Parameters

To configure all ports assigned to a VLAN:

1. Select Configuration from the L2 Switching > VLANs group on the Web Agent window. The VLAN Configuration dialog box opens (Figure 4-1).
2. Click on the Name of the VLAN whose members you want to view. The VLAN Switch Ports dialog box opens (Figure 4-3).

Figure 4-3. VLAN Switch Ports Dialog Box



3. Refer to Table 4-2 to configure the VLAN Switch Ports dialog box parameters:

Table 4-2. VLAN Switch Port Dialog Box Parameters

Parameter	Defines...
Port	The VLAN switch port.
Name	The user-assigned name for this port.

***Table 4-2. VLAN Switch Port Dialog Box Parameters** continued*

Parameter	Defines...
Binding Type	• **Static** - when ports are added manually and can be removed. • **Persistent** - when ports are bound to VLANs automatically but can not be removed. automatically (i.e., if a VLAN Binding for a port is set to 'Bind to All') • **Dynamic** - when port is assigned to VLAN using automatic VLAN binding, which causes ports to bind to VLANs using the Bind to Received switch port setting. The VLAN may be deleted from port, but if VLAN biding is "Bind-to-Receive", the VLAN may be re-added to the port upon receiving tagged traffic. Refer to “Configuring Port VLAN Parameters,” in Chapter 5 for more information.
Frame Format	• **From Port** - causes port to send frames using the frame format specified in the Trunk Mode attribute of the corresponding switch port. **Note:** Refer to “Configuring Port VLAN Parameters,” in Chapter 5 for more information. • **Clear** - causes port to send untagged frames on this port for this VLAN.

4. Click APPLY to save your changes, or CANCEL to restore previous settings.

Creating 3Com Mapping Tables

The Default 3Com Mapping Table maps 3Com VLAN 1 to 16 to the Avaya Default VLAN and 3Com VLANs 2 through 16 to the Avaya Discard VLAN. In a network with multiple 3Com devices, it is possible that some parts of a network will use differentiae VLAN mappings for incoming 3Com tagged packets. The switch allows you to create additional 3Com mapping tables to use in situations where this occurs.

*** Note:** 3Com trunks do not work across hunt groups.

You can create 3Com mapping tables form either the web agent or the CLI.

Creating 3Com Mapping Tables Using the Web Agent

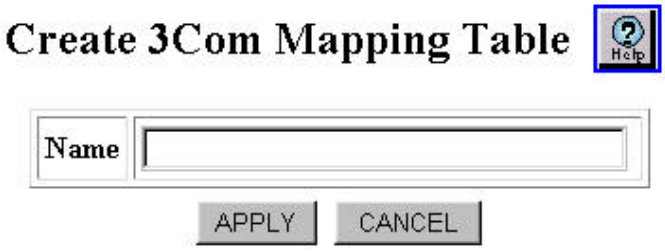
To create additional mapping tables using the web agent:

1. Select 3Com Mapping Table from the L2 Switching > VLANs group on the web agent window. The 3Com Mapping Table Configuration dialog box opens (Figure 4-4).

Figure 4-4. 3Com Mapping Table Configuration Dialog Box (partial view)

2. Select **CREATE**. The **Create 3Com Mapping Table** dialog box opens (Figure 4-5).

Figure 4-5. Create 3Com Mapping Table Dialog Box



3. Enter a name for this entry in the **Name** field.

4. Click APPLY to save your changes, or CANCEL to restore previous settings. The 3Com Mapping Table Configuration dialog box redisplays with the 3Com mapping table name you created listed.

5. Open the corresponding pull-down menus to assign a Avaya VLAN ID association to each of the 16 available VLAN IDs.

6. Click APPLY to save your changes, or CANCEL to restore previous settings.

*** Note:** The mapping instructions in the Default table are fixed and cannot be changed. To actually map VLAN IDs, you must create new 3Com Mapping tables. Setting a port to use a 3Com mapping table causes it to ignore other VLAN tagging parameters. The switch assumes that only 3Com VLAN tags are received on the selected port.

Creating 3Com Mapping Tables Using the CLI

To create additional mapping tables using the CLI, enter the following command in Configure mode:

```
> (configure)# set 3com-mapping-table
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Assigning Ports to VLANs

Refer to “Configuring Switch Port Parameters,” in Chapter 5 for instructions on assigning ports to VLANs.

Using Spanning Tree Setup and Monitoring

Spanning trees are used to prevent loops from forming in your network. The spanning tree algorithm creates a single path through the network by ensuring that if more than one path exists between two parts of a network, only one of these paths is used, while the others are blocked.

*** Note:** You should have a good understanding of the spanning tree protocol (STP) before attempting to configure these parameters. Because of the number of “bridges” present in a switched networking environment, STP structures can become extremely complex. Refer to "Spanning Tree Modes" in Chapter 1.

Managing Spanning Tree

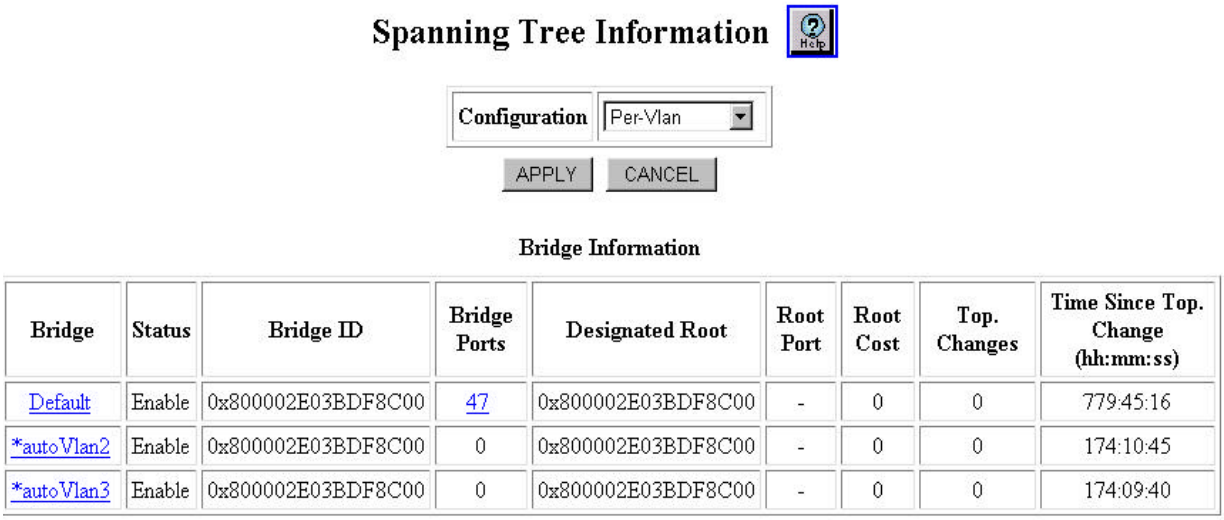
You can manage spanning trees using either the web agent or the CLI.

Managing Spanning Tree Using the Web Agent

To manage spanning tree using the web agent:

1. Select Spanning Tree from the L2 Switching group on the web agent window. The Spanning Tree Information dialog box opens (Figure 4-6).

Figure 4-6. Spanning Tree Information Dialog Box



2. Select the type of spanning tree you want to implement from the Configuration field pull-down menu.

   Refer to Table 4-3 for a definition of the Configuration field parameters:

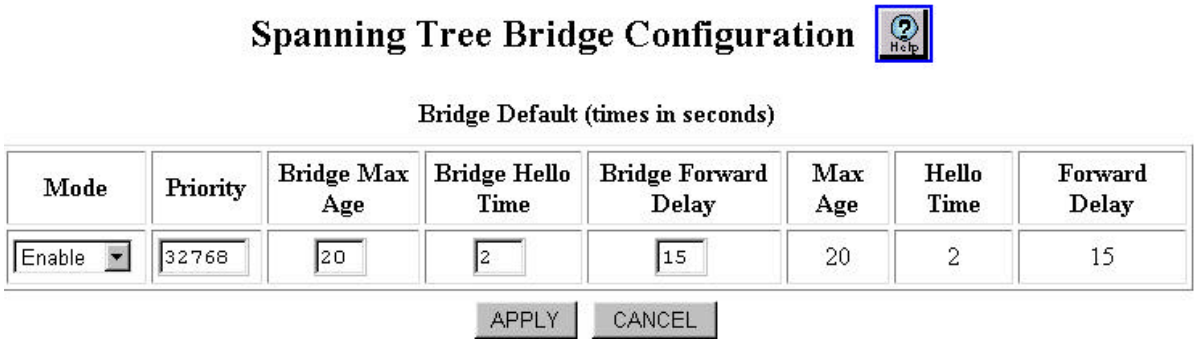
Table 4-3. Spanning Tree Information Configuration Field Options

Parameter	Definition
IEEE 802.1D	Entire switch is a single IEEE 802.1D-compliant bridge. **Note:** When the spanning tree mode is set to IEEE 802.D, BPDUs are sent out ports in Clear (non-trunked) format even if the port has a trunking format (3Com, 802.1Q or Dual layer) defined.
Per VLAN	Each VLAN functions as a separate IEEE 802.1D-compliant bridge. In order for spanning tree to function properly with 3Com trunked ports, the spanning tree mode should be set to per-VLAN. In Per VLAN spanning tree, there is one instance of spanning tree for each VLAN and the BPDUs are tagged with the VLAN ID, ensuring they are interpreted correctly on the receiving end.
Dual Layer	Spanning tree terminates at edge of the switch network. Spanning Tree per VLAN within the switch network.
Disable	Spanning tree not used.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

4. Select a name from the Bridge column to set the bridge parameters. The Spanning Tree Bridge Configuration dialog box opens (Figure 4-7).

Figure 4-7. Spanning Tree Bridge Configuration Dialog Box



5. Refer to Table 4-4 to configure the Spanning Tree Bridge Configuration parameters:

Table 4-4. Spanning Tree Bridge Configuration Parameters

Parameter	Definition
Mode	Determines whether spanning tree is enabled or disabled for this bridge.
Priority	STP Priority level for this bridge.
Bridge Max Age	Sets the maximum amount of time that this bridge retains bridging information before discarding. When the maximum age expires, the bridge assumes it has lost connection to the network, and sends out requests to be re-added to the spanning tree.
Bridge Hello Time	Time between generation of BPDUs by the root bridge.
Bridge Forward Delay	Amount of delay used when a port transitions to the forwarding state. Set by the root bridge for the segment. **Note:** You must enter a value within the supported range or the configuration operation will fail. The supported value range for this parameter is 10-30.
Max Age	Current maximum age for this spanning tree. Determined by the root bridge.
Hello Time	Current hello time for this spanning tree. Determined by the root bridge.
Forward Delay	Current forwarding delay for this spanning tree. Set by the root bridge.

6. Click APPLY to save your changes, or CANCEL to restore previous settings.

Managing Spanning Trees Using the CLI

To manage spanning trees using the CLI, enter the following command from Configure mode:

```
> set spantree config
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring Spanning Tree Bridge Ports

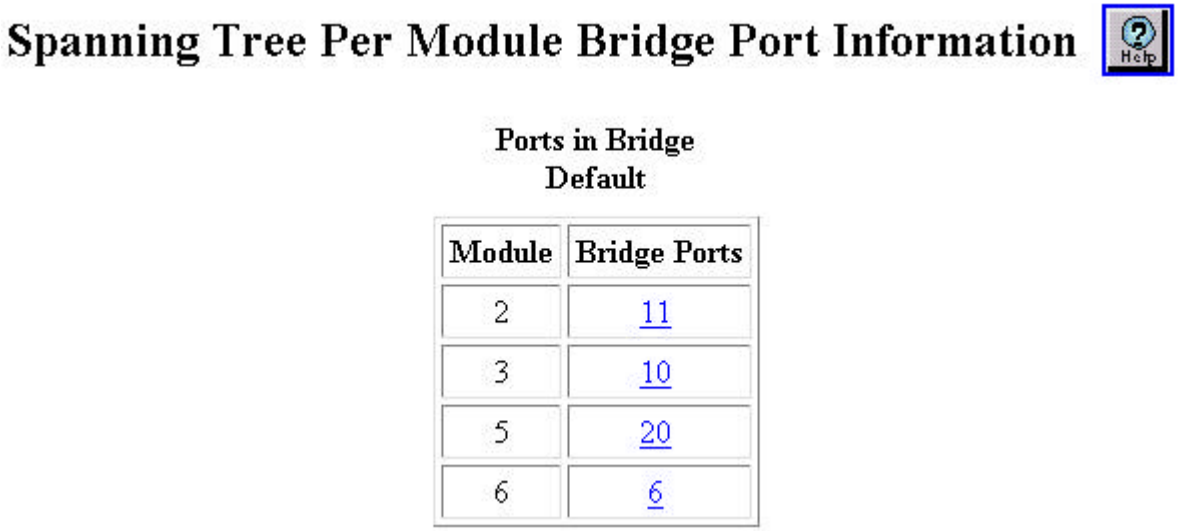
You can configure Spanning Tree Bridge Ports using either the web agent or the CLI.

Configuring Spanning Tree Bridge Ports Using the Web Agent

To configure spanning tree bridge ports using the web agent:

1. Select Spanning Tree from the L2 Switching group on the web agent window. The Spanning Tree Information dialog box opens (Figure 4-6).
2. Select the port number listed in the Bridge Ports column. The Spanning Tree Per Module Bridge Port Information dialog box opens (Figure 4-5).

Figure 4-8. Spanning Tree Per Module Bridge Port Dialog Box



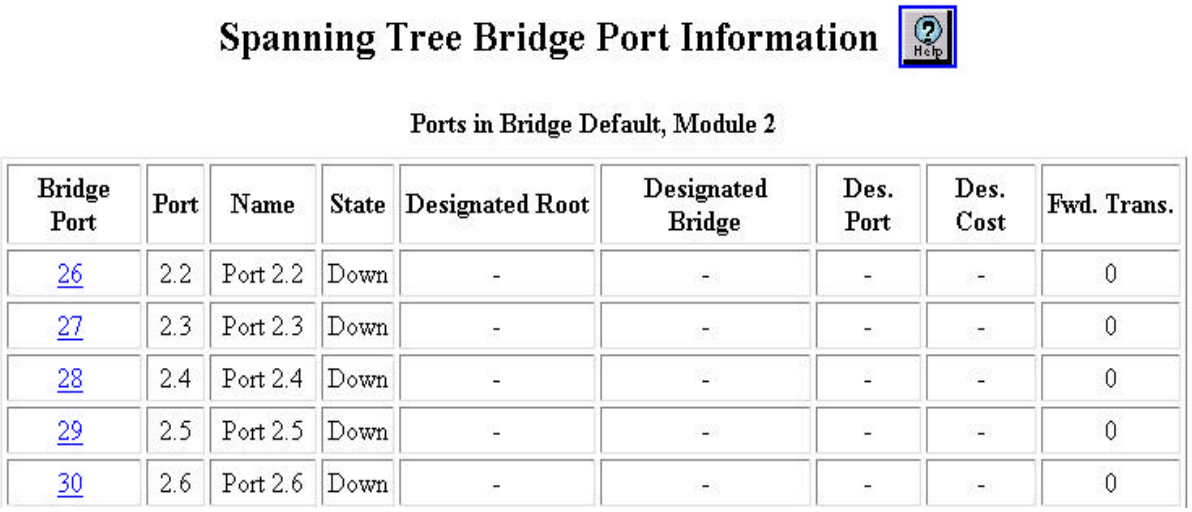
3. Refer to Table 4-5 to configure the Spanning Tree Bridge Port Information dialog box parameters:

Table 4-5. Spanning Tree Bridge Port Information Dialog Box Parameters

Parameter	Options
Bridge Port	The bridge port.
Port	The spanning tree bridge port number.
Name	The name assigned to the bridge port.
State	Current bridging state of the port. The options are: • **Disabled** - The port is disabled. • **Blocking** - The Spanning Tree algorithm has set this port's state to block, meaning that it is enabled, but not passing traffic. • **Listening** - The port is in a transitional state, waiting for the spanning tree algorithm to determine whether it should block or forward traffic. • **Learning** - The port is learning MAC addresses, but not yet forwarding traffic. • **Forwarding** - This port has been selected by the Spanning Tree algorithm to forward traffic, and is forwarding traffic currently. • **Down** - The port's physical port has no link detected.
Designated Root	Displays the Root bridge for this spanning tree.
Designated Bridge	The bridge identifier for the bridge considered to be the designated bridge for this segment.
Designated Port	The port identifier of the port on the designated bridge for this segment of the spanning tree.
Designated Cost	The path cost of the designated root of the segment connected to this port.
Forward Transitions	Number of times that this port has transitioned from blocking to forwarding.

4. Select the Bridge Port number from the Bridge Port column. The Spanning Tree Port Configuration dialog box opens (Figure 4-9).

Figure 4-9. Spanning Tree Bridge Port Information Dialog Box



Spanning Tree Bridge Port Information

Ports in Bridge Default, Module 2

Bridge Port	Port	Name	State	Designated Root	Designated Bridge	Des. Port	Des. Cost	Fwd. Trans.
26	2.2	Port 2.2	Down	-	-	-	-	0
27	2.3	Port 2.3	Down	-	-	-	-	0
28	2.4	Port 2.4	Down	-	-	-	-	0
29	2.5	Port 2.5	Down	-	-	-	-	0
30	2.6	Port 2.6	Down	-	-	-	-	0

5. Refer to Table 4-6 to configure the Spanning Tree Bridge Port Information dialog box parameters:

Table 4-6. Spanning Tree Bridge Port Information Dialog Box Parameters

Parameter	Definition
Enable	Sets whether or not spanning tree is active on this bridge port.
Priority	Sets the port's priority in the spanning tree algorithm. A port with a higher priority (lower priority number) is more likely to be chosen as the primary path in the spanning tree.

***Table 4-6. Spanning Tree Bridge Port Information Dialog Box Parameters** continued*

Parameter	Definition
Path Cost	Sets the spanning tree path cost for this port. The ports that you prefer be used by the spanning tree should have the lowest path cost. **Note:** Configuring the path cost for a link when the link is in the down state is not saved in the configuration NV memory. Establish the link first, before configuring the path cost.
Top. Change Detection	Allows you to enable or disable topology change detection. Specifies whether a Topology Change Notification (TCN) packet is sent through the root port (or if this switch is the root bridge, whether or not Fast Aging occurs) whenever the port enters the forwarding or blocking states. This attribute should only be used on ports which connect to no other switches. **Note:** A topology change occurs when you change a port mirroring piggyback port.

6. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring Spanning Tree Bridge Ports Using the CLI

To configure spanning tree bridge ports using the CLI, enter the following command from Configure mode:

```
> set port spanning-tree-mode {<mod-num>|<mod-swport-
range>}[...,{<mod-num>|<mod-swport-range>}]{disable|enable}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Disabling Spanning Tree Mode for the Port

You can disable Spanning Tree mode for the port from either the web agent or the CLI.

*** Note:** When disabling the STP for a port, BPDUs received on that port are ignored and are not generated. The port moves directly into the forwarding state from the disabled state and does not trigger a topology detection change.

For ports that have a 3Com® trunking format, the receiving end of the trunked port attempts to interpret the clear BPDUs as trunked packets. Consequently, these BPDUs are discarded at the receiving end. For Spanning Tree to function properly with 3Com trunked ports, the Spanning Tree mode should be set to per-VLAN. In per-VLAN Spanning Tree, there is one instance of Spanning Tree for each VLAN and the BPDUs are tagged with the VLAN ID, ensuring they are interpreted correctly on the receiving end.

Although this restriction does not apply to ports that use IEEE 802.1Q or Multi-Layer trunking modes, it is still recommended that you set Spanning Tree to per-VLAN when using trunked ports. This prevents an entire link from being blocked when there is a loop in one VLAN.

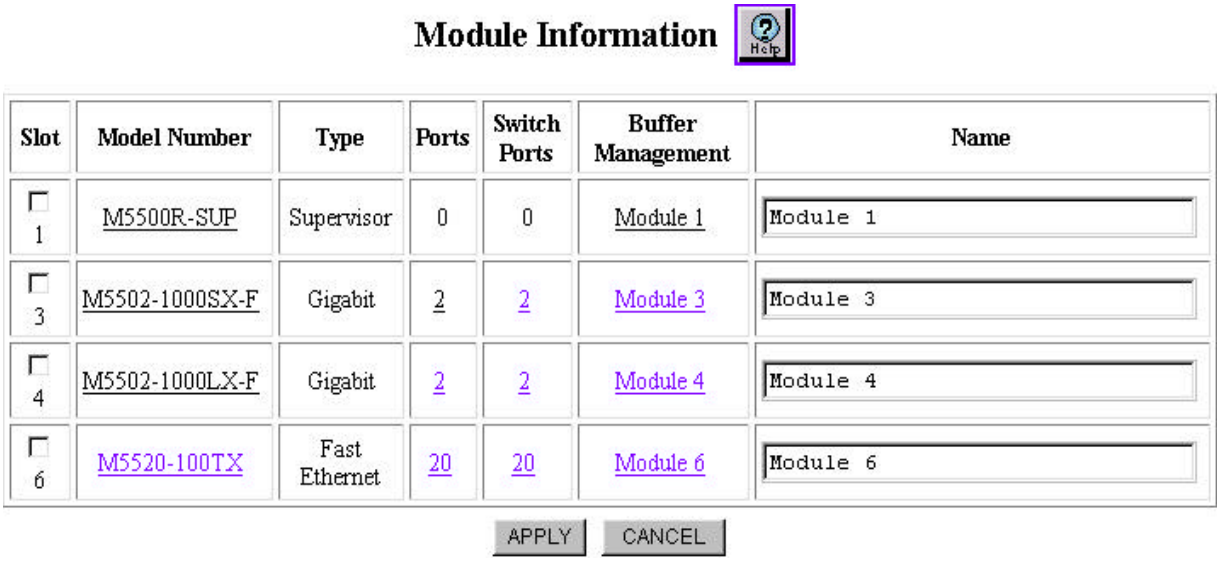
If you have an ATM Uplink module installed, and there is a loop through the uplink, the ATM Uplink module does not function properly if you use IEEE802.D.

Disabling Spanning Tree Mode for the Port Using the Web Agent

To disable spanning tree mode for the port using the web agent:

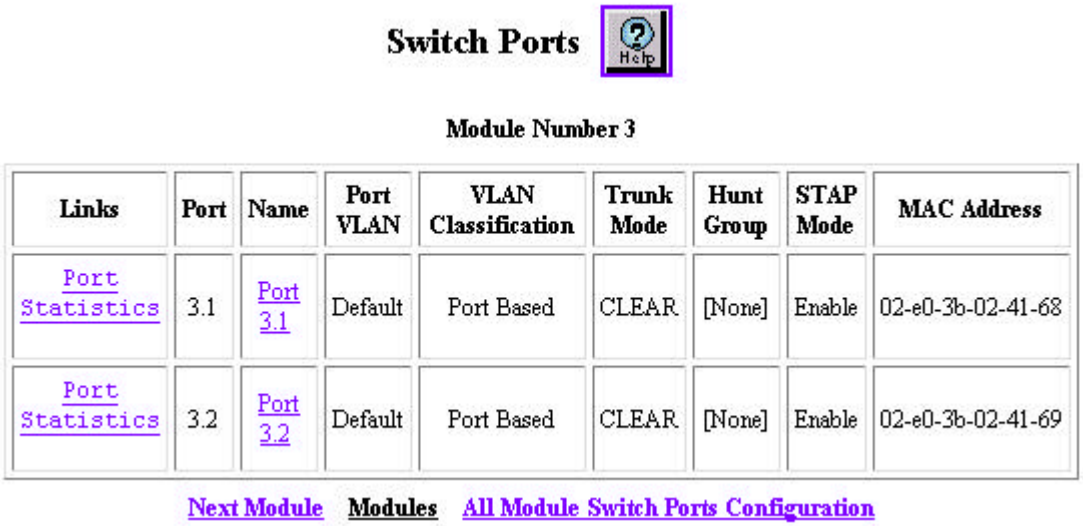
1. Select Configuration from the Modules and Ports web agent window. The Module Information dialog box opens (Figure 4-10).

Figure 4-10. Module Information Dialog Box



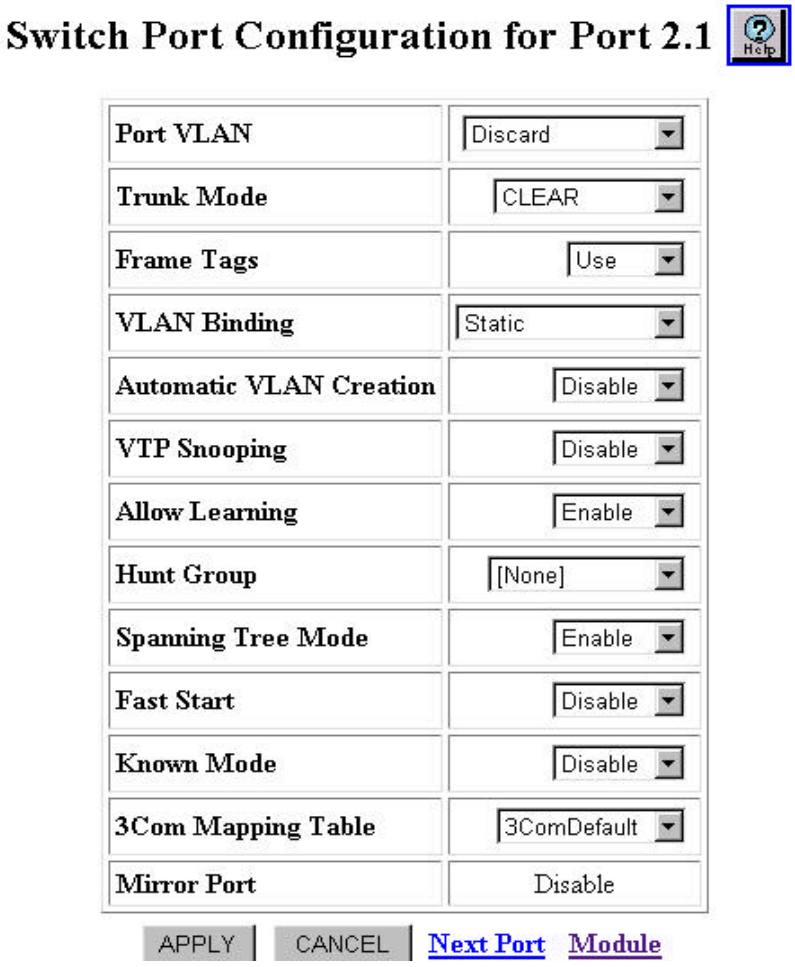
2. Select the switch port number from the Switch Ports column. The Switch Ports dialog box opens (Figure 4-11).

Figure 4-11. Switch Ports Dialog Box



3. Select the port number on which you want to disable spanning tree from the Name column. The Switch Port Configuration dialog box for that port opens ((Figure 4-12).

Figure 4-12. Switch Port Configuration Dialog Box



4. Select Disable from the Spanning Tree Mode pull-down menu.

5. Click APPLY to disable spanning tree mode on the port, or CANCEL to keep spanning tree mode Enabled on the port.

Disabling Spanning Tree Mode on a Port Using the CLI

To Disable Spanning Tree mode on a port using the CLI, enter the following command from Configure mode:

```
> set port spanning-tree-mode <mod-num> disable
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Using Hunt Groups to Aggregate Bandwidth between Switches

Hunt groups allow you to aggregate multiple switch ports into a single group, effectively combining the bandwidth into a single connection.

For example, if you connect three gigabit ports each on a pair of switches into a hunt group, the aggregated connection will have six gigabits of available bandwidth (full- duplex).

Hunt groups also provide fault tolerance. If a port in a hunt group fails, the remaining ports will continue forwarding the traffic on the link.

Features

Hunt group features include:

- Shared traffic load.
- Address-based traffic sorting — This keeps packets in the right order.
- Fault tolerance — If a port in a group fails, the remaining ports in the group pick up the traffic load.
- Support for any number of same-speed connections in a group — The group is not restricted to a single module in a switch.
- Quicker recovery from link failure — If a port in the group fails, the remaining ports carry the load. Recovery is not limited by STP convergence time (convergence time is the time the network takes to resume steady-state forwarding after STP reconfiguration).
- Supports up to 25 groups per switch.

How Hunt Groups Load Share

Hunt Groups load share by allowing different users to use different ports on the hunt group when sending traffic to a particular user. Broadcasts and Destination Unknown Unicasts traverse the flood port (also referred to as the base port).

To understand how load sharing works with the hardware, one must understand the relationship between users, I/O cards, Fabric Ports and Packet Lookup Engines (PLEs). For the P550, there are two fabric ports per I/O slot (slots 2 through 7) and one fabric port for the CPU slot (slot 1). There is generally one PLE per fabric port for a layer 2 Card and two PLE's per fabric port for a layer 3 Card (with the exception of the 4 port Gigabit Ethernet Card which has one PLE per port). Each I/O card uses the two fabric ports in the slot with the exception of the 10 Port 100FX card and the 12 port 10/100 card which only use one fabric port in the slot. Table 4-7 lists the number of PLEs and fabric ports for the various modules supported by the Cajun switch.

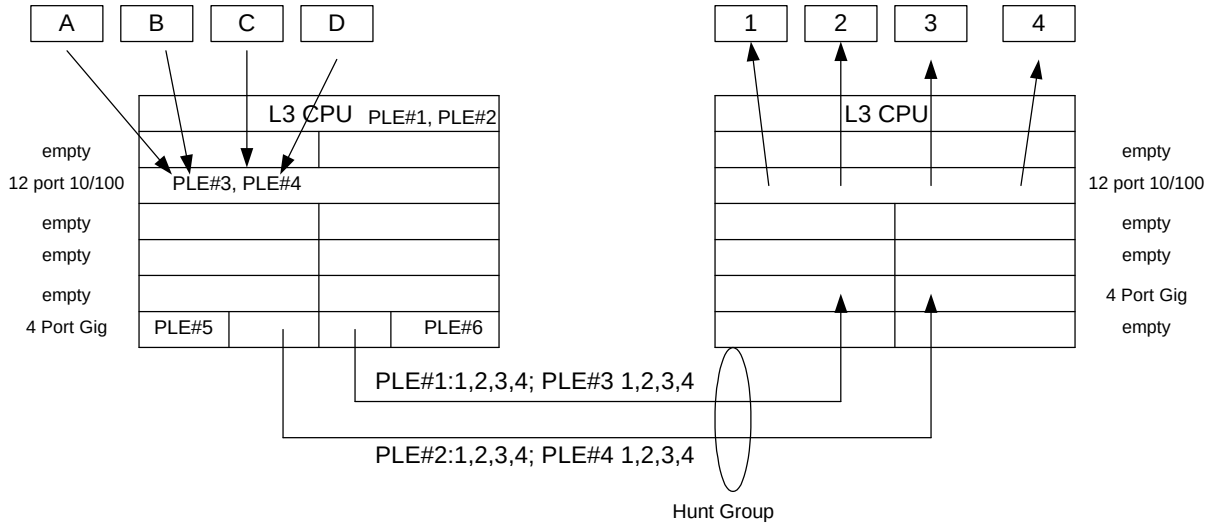
Table 4-7. Module PLEs and Fabric Ports

Module Type	Total Number of PLEs	Number of Fabric Ports	Description
M5500	0	1	
M5500R	2	1	FORE port, CPU
10 Port FX (layer 2)	1	1	
10 Port FX (layer 3)	2	1	
12 Port TX (layer 3)	2	1	
2 Port Gigabit (layer 2)	2	2	
2 Port Gigabit (layer 3)	4	2	
4 Port Gigabit (layer 2)	4	2	2 per fabric port, 1 per port
20 Port TX (layer 2)	2	2	

Note: All layer 3 I/O modules have a pre-L3 path PLE, and a PLE in the L3 path.

Figure 4-13 shows an example of a Hunt group load share.

Figure 4-13. Load Sharing Example

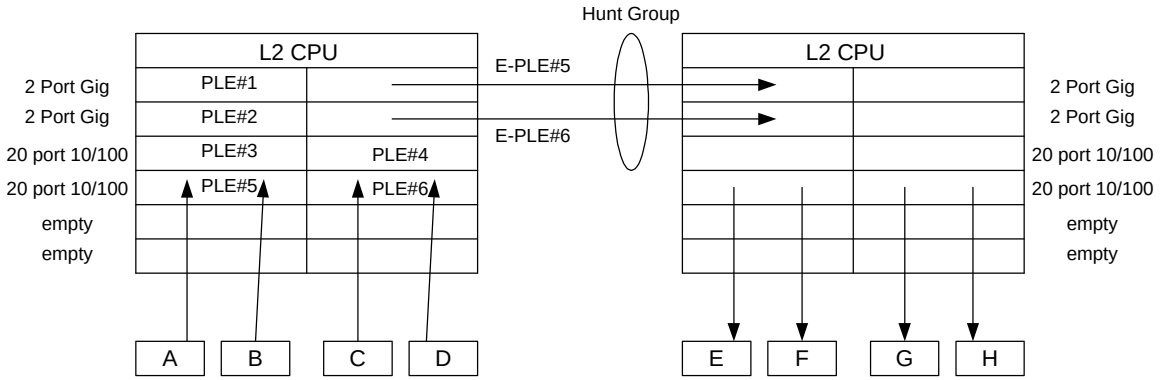


The first two users on each switch are connected to one of the ports in the 1 through 10 range on the 20 port 10/100 card. The second two users on each switch are connected to one of the ports in the range 11 through 20 on the 20 port 10/100 cards. There are 6 PLEs in this configuration. This does not include the PLE's associated with the two Hunt Group ports which are labeled 1 through 6.

Load sharing is done in a round-robin fashion based upon BOTH the Destination MAC Address and the Source PLE. The links on which unicast packets traverse to reach User E depends upon the source user's associated PLE. Users A and B are associated with PLE#5 and therefore the first link in the Hunt group will be used for unicast packets from A to E and from B to E. Users C and D are associated with PLE#6 and therefore the second link in the Hunt Group will be used for unicast packets from C to E and D to E.

Figure Figure 4-14 illustrates how the P550 distributes it PLEs to load-share hunt group traffic.

Figure 4-14. Load Sharing PLEs



The P550 uses its distributed PLEs to load-share hunt group traffic. The PLEs are categorized into two groups:

- member PLE
- non-member PLE

Member PLE's service traffic sourced from a particular hunt group. Members are restricted to selecting one port for all hunt group related traffic. This port is called the "base" port. This restriction prevents the system from receiving spurious learn events.

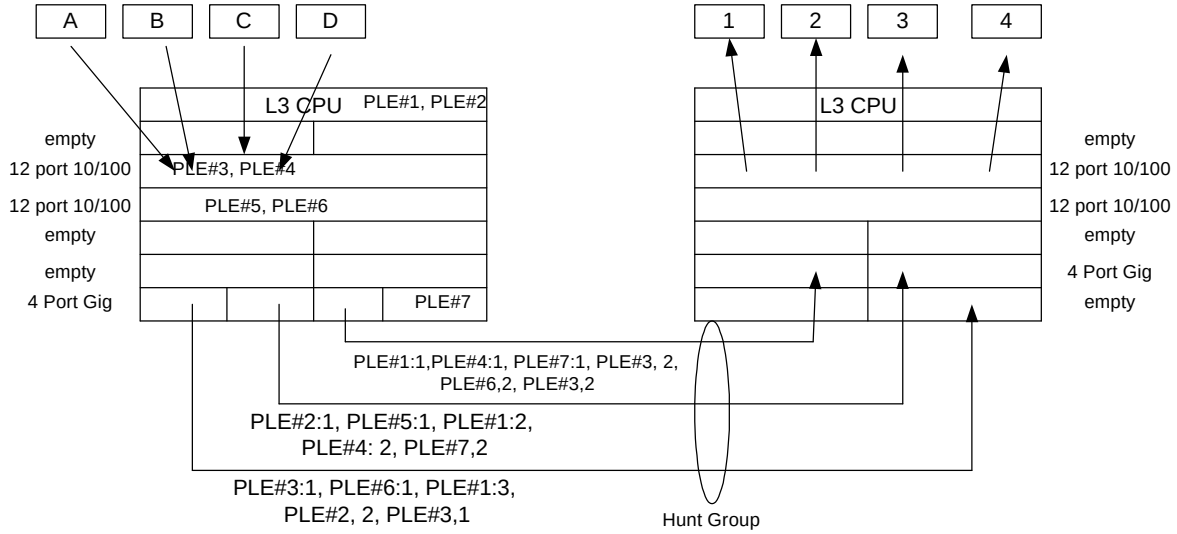
Non-member PLE's do not service traffic sourced from a particular hunt group and therefore are free to select any port for hunt-group destined traffic. The hunt group port that is selected is based on the source PLE and the destination MAC address. Before this enhancement, all non-member PLEs chose the same port for a given destination address. Now, non-member PLEs choose different ports (modulo the total number of ports in the hunt group) for a given destination address.

Hunt group ports should be segregated from the ports involved in traffic flows to the hunt group with respect to the PLE's servicing those ports. The greater the number of non-member PLEs in the system, the greater the ability of the system to load-share.

There are six Non-Member PLEs (the 12 port is associated with a single fabric port but has two PLEs – one in the routing path and one before the routing path, and the 4 port has a PLE per port). Load sharing is now accomplished by Destination MAC Address and Source PLE. When Mac Address 1 is learned, it is assigned to the first Hunt Group link for PLE#1, the second for PLE#2, the first for PLE#3, the second for PLE#4, the first for PLE#5 and the second for PLE#6. The second MAC Address is round-robin assigned in the same fashion and so on. Since the number non-member PLEs is divisible by the number of ports in the hunt group – load sharing does not occur when ALL traffic is sourced from the same PLE (e.g. all PLE#1 unicast packets traverse the same link).

Figure 4-15 shows a second load-sharing example.

Figure 4-15. Load-Sharing Example 2



In Figure 4-15, the first MAC Address is assigned to the first port in the Hunt Group for PLE #1, the second port in the Hunt Group for PLE#2, the third port in the Hunt Group for PLE#3, the first port in the hunt group for PLE#4, the second port in the Hunt Group for PLE#5, the third port in the Hunt Group for PLE#6, and the first port in the Hunt Group for PLE#7.

The second MAC Address is then learned on the second port in the hunt group for PLE#1, the third port in the Hunt Group for PLE#2, the third port in the Hunt Group for PLE#3, the fourth port in the hunt group for PLE#4, and so on. The load sharing problem is alleviated even though all traffic is the sourced from the same PLE (data from PLE#1 is split between the three links). Since the case in Figure 4-5 is not expected in live networks, it is not viewed as a serious issue with the P550 hunt group implementation.

Hunt Group Considerations

Consider the following before creating hunt groups:

- When creating a hunt group, you have to verify that the ports in a group on one switch are physically connected to the ports in that group on the other switch. The switches do not yet have a link discovery protocol.
- If one end of a connection is in a hunt group, the other end of the connection should also be in a hunt group. If you don't do this, the forwarding behavior of the hunt group will be unpredictable.
- You should disable or disconnect the ports in a hunt group until both ends of the link are configured.
- All ports in a hunt group should be the same speed and the same media type (Layer 2 and Layer 3).
- Packets arriving on different fabric ports within the switch will have loads balanced more evenly.
- Hunt groups will not load share if the source and destination traffic and the hunt group ports are on the same fabric port. Most I/O modules divide their ports evenly across two fabric ports. For 10-port and 12-port I/O modules, all ports use a single fabric port.
- The first port assigned to a hunt group becomes the flood port. It cannot be changed unless the flood port is disabled.
- 4-port and 2-port Gigabit Ethernet modules, and layer 2 and layer 3 modules cannot share the same Hunt group.

Creating Hunt Groups

You can create hunt groups from either the web agent or the CLI.

Creating Hunt Groups Using the Web Agent

To create a hunt group using the web agent:

1. Check the speed of the ports that you are configuring into the hunt group. The ports must be physically connected to each other (for example, in a four-port gigabit hunt group, ensure that you have four fiber cables with switch ports connected at each end).

   ***Note:** Auto-negotiation should be disabled on the ports to further insure against speed mismatch.

2. Select Configuration from the Modules and Ports group on the Web Agent window. The Module Information dialog box opens (Figure 4-16).

Figure 4-16. Module Information Dialog Box.

Module Information

Slot	Model Number	Type	Ports	Switch Ports	Buffer Management	Name
☐ 1	M5500R-SUP	Supervisor	0	0	Module 1	Module 1
☐ 3	M5502-1000SX-F	Gigabit	2	2	Module 3	Module 3
☐ 4	M5502-1000LX-F	Gigabit	2	2	Module 4	Module 4
☐ 6	M5520-100TX	Fast Ethernet	20	20	Module 6	Module 6

APPLY CANCEL

3. Select a port number from the Ports column. The Physical Port Configuration dialog box opens (Figure 4-17).

Figure 4-17. Physical Port Configuration Dialog Box.

Physical Port Configuration - Module 6

Port	Name	Enable	Status	Type	Connector	Auto Negotiation Mode	Speed State	Duplex State	Flow Control State
6.1	Port 6.1	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.2	Port 6.2	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.3	Port 6.3	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.4	Port 6.4	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.5	Port 6.5	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.6	Port 6.6	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled

4. Select a checkbox from the Enable column for a specific port. This disables that port. The checkmark disappears and the port is disabled.

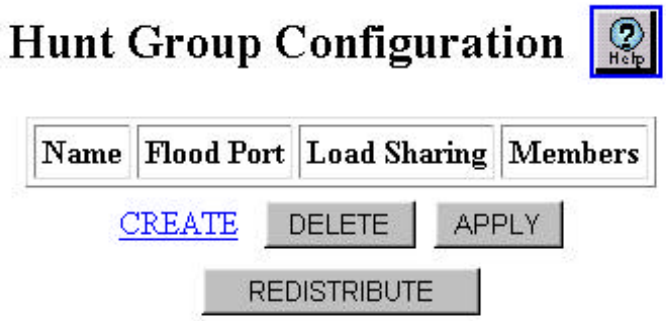
   — If this is a new hunt group, disable all of the ports you are adding to the hunt group.

   — If you are adding ports to an existing hunt group, disable the ports you are adding.

5. Click Apply to save your changes.

6. Select Hunt Groups from the L2 Switching group in the web agent window. The Hunt Group Configuration dialog box opens (Figure 4-18).

Figure 4-18. Hunt Group Configuration Dialog Box.



7. Select CREATE. The Create Hunt Group dialog box opens (Figure 4-19).

Figure 4-19. Create Hunt Group Dialog Box.

8. Enter a name for the hunt group in the Name field,.
9. Select Enable from the Load Sharing pull-down menu to enable the Hunt Group.
10. Click APPLY to save your changes, or CANCEL to restore previous settings.

Creating Hunt Groups Using the CLI

To create a hunt group using the CLI, enter the following command from Configure mode:

```
> set huntgroup <huntgroup-name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Viewing Hunt Group Members

You can view Hunt Group members from either the web agent or the CLI.

Viewing Hunt Group Members Using the Web Agent

To view details about hunt group members using the web agent:

1. Select Hunt Groups from the L2 Switching group in the web agent window. The Hunt Group Configuration dialog box opens (Figure 4-18).
2. Select a highlighted number in the Members column. The Hunt Group Members dialog box opens with pertinent information about the members of that hunt group (Figure 4-20).

Figure 4-20. Hunt Group Members Dialog Box.

Viewing Hunt Group Members Using the CLI

To view details about hunt group members using the CLI, enter the following command in Priv mode:

```
> show huntgroup <huntgroup-name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Adding Ports to a Hunt Group

You can add ports as needed after you create a hunt group. You can add ports using either the web agent or the CLI.

Adding Ports to a Hunt Group Using the Web Agent

To add ports to a hunt group using the web agent:

1. Select Configuration from the Modules and Ports group on the Web Agent window. The Module Information dialog box opens (Figure 4-16).
2. Select a port number from the Ports column. The Physical Port Configuration dialog box opens (Figure 4-17).
3. Select a checkbox for a specific port from the Enable column. This disables that port. The checkmark disappears and the port is disabled.
4. Click APPLY to save your changes, or CANCEL to restore previous settings.
5. Select Modules at the bottom of the Physical Port Configuration dialog box. The Module Information dialog box re-opens.
6. Select a number from the Switch Ports column for the module whose port(s) you are adding to the hunt group. The Switch Ports dialog box opens (Figure 4-21).

Figure 4-21. Switch Ports Dialog Box

Switch Ports Help

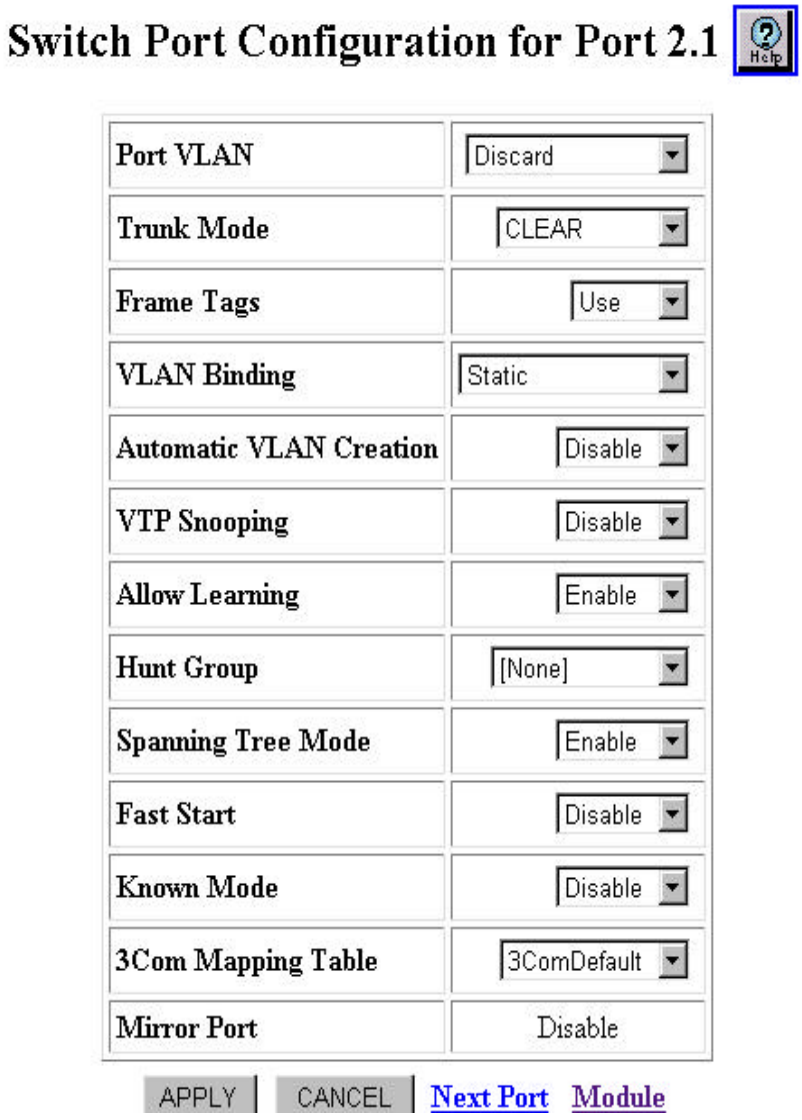
Module Number 3

Links	Port	Name	Port VLAN	VLAN Classification	Trunk Mode	Hunt Group	STAP Mode	MAC Address
Port Statistics	3.1	Port 3.1	Default	Port Based	CLEAR	[None]	Enable	02-e0-3b-02-41-68
Port Statistics	3.2	Port 3.2	Default	Port Based	CLEAR	[None]	Enable	02-e0-3b-02-41-69

Next Module **Modules** All Module Switch Ports Configuration

7. Select the name of the port you want to configure from the Name column. The Switch Port Configuration dialog box for that switch port opens (Figure 4-22).

Figure 4-22. Switch Port Configuration Dialog Box.



8. Select the trunk group assignment of the port from the Trunk Mode pull-down menu. Options are IEEE 802.1Q, Multi-Layer, and 3Com.

9. Click APPLY to save your changes, or CANCEL to restore previous settings.

10. Repeat Steps 1-9 for any additional ports that you want to add to this hunt group.

11. Repeat steps 1 through 10 on the switch at the other end of the hunt group connection.

12. Select Configuration from the Modules & Ports group on the web agent window. The Module Information dialog box re-opens (see Figure 4-16).

13. Select a port number from the Ports column. The Physical Port Configuration dialog box opens (see Figure 4-17).

14. Select a checkbox from the Enable column for that port. The group can now function as a load-sharing connection.

15. Click APPLY to save your changes, or CANCEL to restore previous settings.

*** Note:** If thousands of addresses have been learned on a port and a link in the hunt group goes down, the switch-over of traffic between ports may take several seconds.

Adding Ports to a Hunt Group Using the CLI

To add ports to a hunt group using the CLI, enter the following command from Configure mode:

```
> (configure)# set port huntgroup
{<mod-num>|<mod-swport-range>}
[...,{<mod-num>|<mod-swport-range>}]<huntgroup-
name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring VLAN Trunk Protocol (VTP) Snooping

VTP is a layer 2 protocol developed by Cisco to maintain VLAN configuration consistency among its switches. VTP only runs over trunk ports that have enabled either Cisco Inter-Switch Link (ISL) or IEEE 802.1Q tagging. By using VTP snooping, you can allow your Cajun switch to synchronize its VLAN configuration with that of a Cisco switch that is running VTP in the same network.

VLAN additions, deletions, and name changes made on the network's Cisco VTP server are automatically updated on Cajun switches that have VTP Snooping enabled and are connected to the Cisco VTP server. VLAN changes made on a Cajun switches are not automatically updated on any other switch.

*** Note:** VTP Snooping is **Disabled** by default. You only need to change VTP Snooping port settings if you want to Enable its ability to learn VLAN changes on a Cisco VTP server.

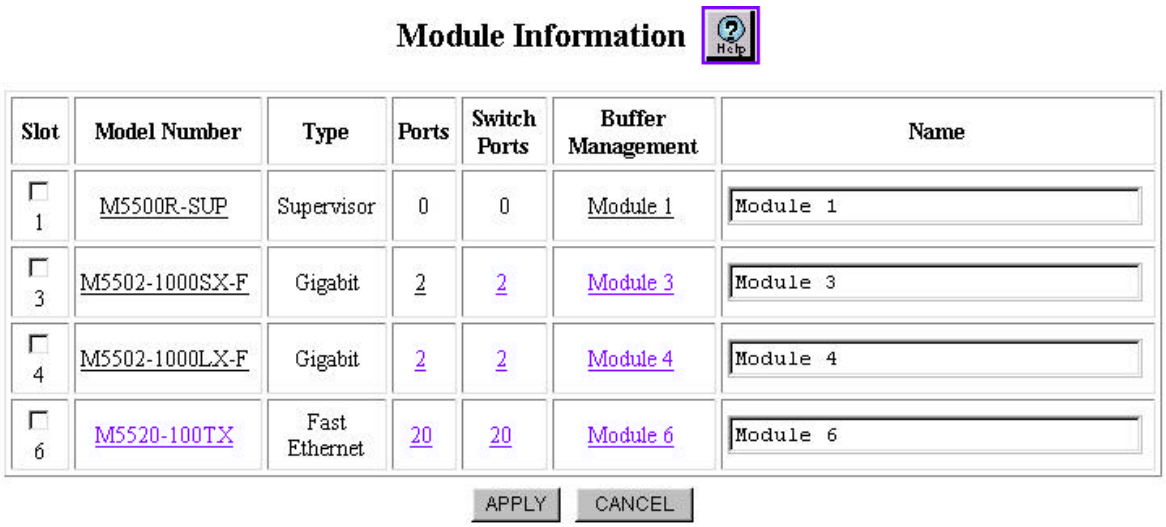
You can configure VTP snooping using either the web agent or the CLI

Configuring VTP Snooping Using the Web Agent

To configure VTP snooping using the web agent:

1. Select Configuration from the Modules & Ports group on the web agent window. The Module Information window opens (see Figure 4-23).

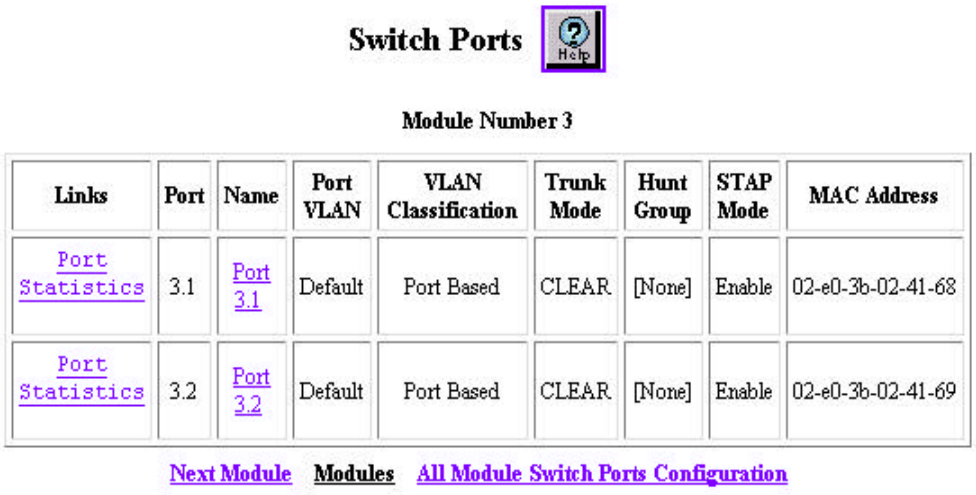
Figure 4-23. Module Information Window



2. Select the checkbox in the Slot column for the module on which you want to configure VTP snooping.

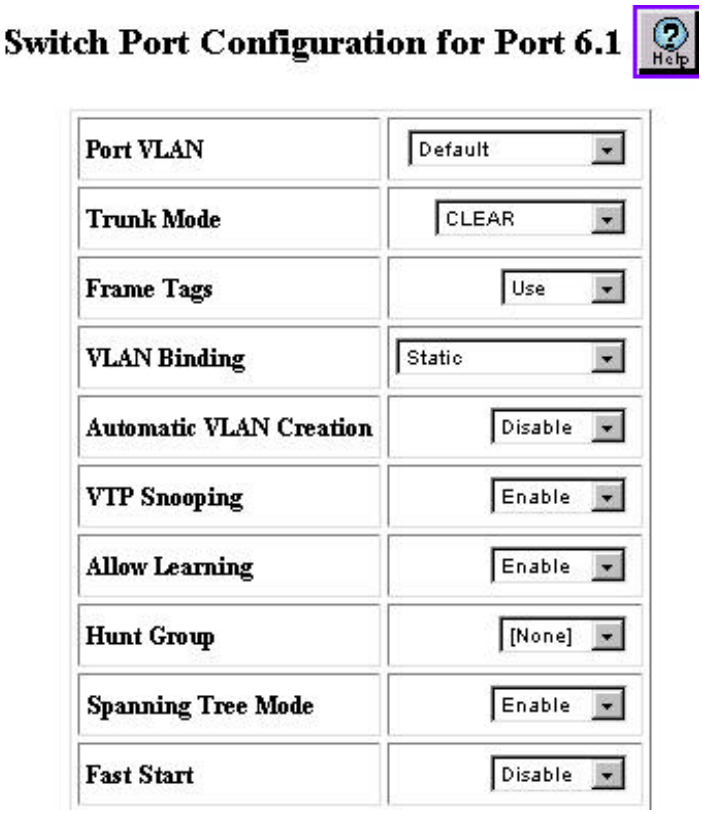
3. Select the number in the Switch Ports column for that module. The Switch Ports dialog box for that module opens (see Figure 4-24).

Figure 4-24. Switch Ports Window



4. Select the port in the Name column on which you want to enable VTP Snooping throughout the switch. The Switch Port Configuration window opens for that port (see Figure 4-25).

Figure 4-25. Switch Port Configuration Window with VTP Options



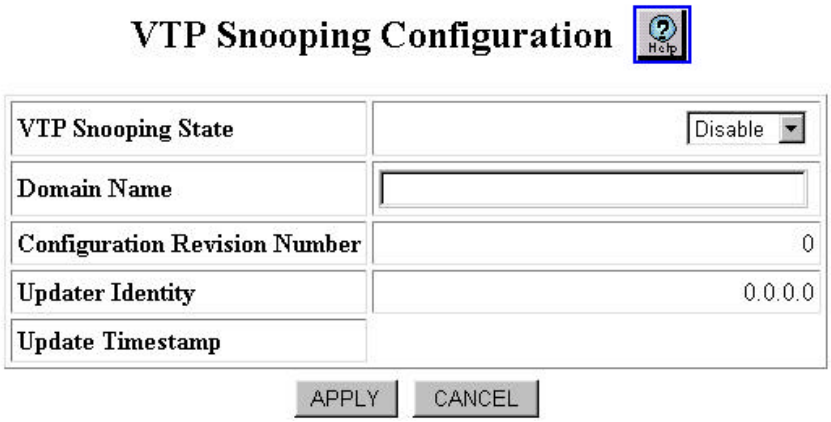
5. Select either IEEE 802.1Q or Multi-layer from the Trunk Mode pull-down menu to match the setting of the trunk mode for the switch port at the other end of the link.

6. Select Enable from the VTP Snooping pull-down menu. This enables VTP snooping on the switch.

7. Click APPLY to save your changes, or CANCEL to restore previous settings.

8. Select VTP Snooping from the L2 Switching > VLANs group on the web agent window. The VTP Snooping Configuration window opens (see Figure 4-26).

Figure 4-26. VTP Snooping Configuration Window



9. Refer to Table 4-8 and configure the VTP Snooping parameters.

Table 4-8. VTP Snooping Parameters

Parameter	Definition
VTP Snooping State	Select to **Enable** to enable VTP snooping globally for the switch. The default value is **Disable**.
Domain Name	Enter the name associated with the Cisco VTP domain. The default is Null. **Note:** The domain name is automatically learned from a Cisco VTP switch provided both the Domain Name is Null and the VTP Snooping State is enabled on the Cajun switch.
Configuration Revision Number	Displays the VTP snooping configuration revision number associated with the last successful VTP configuration update on the Cajun switch.
Updater Identity	Displays the IP address of the Cisco switch that initiated the configuration update.
Update Timestamp	Displays the date and time that the Cisco switch initiated the configuration update.

10. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring VTP Snooping Using the CLI

To configure VTP snooping using the CLI, enter the following command in Configure mode:

```
> (configure)# set vtp-snooping enable
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

5 Configuring Port Parameters

Overview

The following information and procedures are provided in this chapter and are common to both layer 2 and layer 3 module configuration:

- Configuring Port Parameters
- Physical Port Features
- Switch Port Features
- Configuring Physical Port Parameters on Gigabit Ports
- Configuring Physical Port Parameters on Fast Ethernet Ports
- Using the All Ports Configuration Window
- Viewing Switch Port Parameters
- Configuring Switch Port Parameters
- Configuring Port VLAN Parameters
- Configuring Non-VLAN Switch Port Parameters

Configuring Port Parameters

The system has two levels of port settings:

- **Physical port parameters** — Allows you to set up rules that guide the system's physical layer interaction (for example, enable/disable, speed, auto-negotiation).
- **Switch port parameters** — Allows you to specify how the port participates in switching (for example, VLAN mode, trunking).
- **Buffer Management** — TBD, NEEDS TO BE WRITTEN

The following sections explain some of the Cajun P550/P880 features and how to configure the switch ports.

Physical Port Features

This section describes the following features that are available when configuring the physical parameters on the ports:

- Autonegotiation
- Flow Control

Auto-negotiation

Autonegotiation is an extension of the link test methods used by 10Base-T and 10Base-FL to verify the integrity of the link between devices. Autonegotiation advertises a device's abilities by encoding a 16-bit data packet, called a link code word (LCW), within a burst of 17 to 33 link pulses, called a fast link pulse (FLP) burst. FLP bursts have an approximate duration of 2 µs and are transmitted in 16.8 µs intervals (the same interval as for the normal link pulses used by 10Base-T and 10Base-FL).

However, this does not hold true for the Half Duplex/Full Duplex (HD/FD) selection. If a non-autonegotiating device running FD is connected to a negotiating device, the negotiating device runs at HD, and the link does not operate properly.

*** Note:** A Gigabit Ethernet device negotiates at HD or FD, not speed.

The LCW contains two fields (the selector field and the technology ability field), which together serve to identify a device's capabilities.

It may seem that because the FLP and the normal link pulse use the same interval at the same frequency, older devices may not be compatible with auto-negotiation. This is, however, not the case. For example, a 10Base-T device that does not have auto-negotiation capabilities sees FLP bursts simply as a link test signal. A 10Base-T device will respond to the FLP burst with its usual normal link pulse signal. At the other end of the link, a 10/100-capable device will recognize normal link pulse and choose 10Mbps mode operation.

Auto-negotiation attempts to find the greatest common denominator for the two devices on the link in the following order of preference:

1. 100Base-TX full-duplex
2. 100Base-T4
3. 100Base-TX
4. 10Base-T full-duplex
5. 10Base-T half-duplex

Once the greatest common denominator of settings is determined, each device equipped with auto-negotiation will configure itself automatically. In certain cases where automatic configurations are not desired, auto-negotiation provides a way for these settings to be overridden manually.

Flow Control

There are three flow control options on 10/100 Ethernet ports:

1. Disable,
2. Enable,
3. Enable with Aggressive Backoff.

There are four flow control options on Gigabit Ethernet Ports.

1. Disable,
2. Enable,
3. Enable – Send Only
4. Enable – Respond Only

The "Disable" option disables flow control (the default).

The "Enable" option enables IEEE802.3X (XOFF/XON) Flow Control on the line. We are the Sender of pauses based upon inbound traffic and we are the receiver of pauses based upon outgoing traffic (and the ability of attached equipment to use the protocol).

With Gigabit links, you can:

- Enable IEEE802.3X for both send and receive (the "Enable" setting)
- Only send pause (XOFF/XON) signals (the "Enable – Send Only" option)
- Only respond to the pause signals (the "Enable – Respond Only" option).

With 10/100 links you can use the "Enable with Aggressive Backoff" option to enable Active Backpressure (creation of a collision) on a link. Active Backpressure only applies to HD links so that when a 10/100 link is in FD, options 2 and 3 are identical.

Refer to Table 5-1 lists the gigabit modules that do not support autonegotiation:

Table 5-1. Gigabit Modules not Supporting Autonegotiation

Gigabit Module Model Number	Hardware Revision
M5502-1000SX-F	M or earlier
M5502-1000LX-F	M or earlier
M5502-1000SLX-F	F or earlier
M5504-1000SX-F	H or earlier
M5504-1000LX-F	H or earlier
M5504-1000SLX-F	H or earlier
M5502R-1000SX-F	J or earlier
M5502R-1000LX-F	J or earlier
M5502R-1000SLX-F	H or earlier

*** Note:** If a Gigabit module that does not support the autonegotiation is connected to a device that does, disable autonegotiation to ensure proper operation.

If you enable flow control, the switch manages the inbound buffers with flow control (IEEE 802.1X XOFF, or Backpressure) applied when a high water mark is reached. thus, no matter which flow control option is chosen, outgoing pauses or backpressure are only applied to the port on which the parameter is set based upon the inbound traffic for that port in the default queuing mode.

Flow control is not applied across the switch itself. Therefore, if you have a server sending data on one port at 100MB and a client receiving the data at 10MB, the switch will not throttle the data at the Server's input based on outgoing buffer backup on the client's port in this default queuing mode.

Switch Port Features

The P550/P880/P882 switches all support up to 1024 VLANs and also supports multiple forwarding databases. This means that each VLAN is associated with its own Address Forwarding Table (AFT). Therefore, identical MAC addresses can simultaneously exist on multiple VLANs. The P550/P880/P882 switches have many parameters for configuring VLAN/port associations.

This section provides the following:

- Creating Virtual LANs (VLANs)
- VLAN Operational Rules
- Relationship Between Different Switch Port Parameters
- Assigning VLANs to a Port and Associated Issues

Creating Virtual LANs (VLANs)

A VLAN is a logical network that consists of one or more ports from one or more switches that are logically grouped together. The advantage of using VLANs is threefold:

- Broadcast and multicast containment
- Increased network bandwidth
- Logical workgroups can share network resources

You can create VLANs manually and automatically on the P550/P880/P882 switch.

Manual VLAN Creation

The manual creation of VLANs is done through the 'Virtual LANs' menu selection. When a VLAN is created manually, the user assigns a VLAN name and VLAN ID to each VLAN that is created. VLAN names and VLAN Ids must be unique for each VLAN created within a P550/P880. To make ports on more than one device participate in a particular VLAN, you must use the same VLAN ID to identify the VLAN on every device.

Automatic VLAN Creation

Automatic VLAN creation is done by enabling the 'Automatic VLAN Creation' parameter on an individual port under the 'Module & Ports' menu. With this parameter enabled, the port will automatically create a VLAN each time it receives a frame from an unknown VLAN ID in received IEEE 802.1Q and Multi-Layer tagged frames.

*** Note:** The automatic VLAN creation feature does not create entries in 3Com Mapping Tables.

When a VLAN is created automatically the VLAN name and VLAN ID are derived from the received tagged frame. The VLAN name will be created as "*autoVlan [VLAN ID]". The VLAN ID will be identical to the VLAN ID of the received tagged frame. As with all VLANs, the VLAN name may be modified to something more descriptive.

Refer to Table 5-2 shows the P550/P880/P882 switch VLAN table. The VLANs 'Default' and 'Discard' are permanent VLANs assigned to every switch. VLAN 'Net90' is a manually created VLAN, while VLAN '*autoVlan1001' was created automatically by software.

Table 5-2. P550/P880/P882 Switch VLAN Table.

Name	ID	Group ID	AFT Index
Default	1	2	1
Discard	8193	3	3
*Net90	90	90	7
**autoVlan1001	1001	1001	11

* Created manually
** Automatically created by the switch software

Automatically Creating VLANs and Frame Tags Parameters

VLANs are created automatically by the switch reading the VLAN tag of all ingress IEEE 802.1Q and Multi-Layer tagged frames. The switch then creates a new VLAN for every new VLAN tag identified. However, if the parameter for 'Frame Tags' is set to "ignore", the switch will ignore the VLAN tags on ingress frames. The switch assumes that all ingress frames belong to the 'Port VLAN'. Therefore, no new VLANs will ever be created automatically.

Automatic Binding of VLANs to Ports

When a VLAN is either manually or automatically created, the software may automatically bind the VLAN to a port depending on the setting of the ‘Trunk Mode’ parameter assigned to the port.

- When a VLAN is created manually the software assigns the VLAN to all ports whose ‘Trunk Mode’ is set to ‘Bind-to-All’. No other ports will automatically be assigned when a VLAN is created manually.
- When a VLAN is created automatically the software assigns the VLAN to the port it is received on if that port is set to 'Bind-to-All' and 'Bind-to-Received". Additionally, software will assign the VLAN to all other ports whose 'Trunk Mode' is set to 'Bind-to-All'. No other ports will automatically be assigned when a VLAN is created manually.

VLAN Operational Rules

VLANs are limited by physical switch domains. Users in various physical locations that belong to the same workgroup can participate in the same VLAN or multiple VLANs, as required. This helps simplify network resource management.

VLAN Operation are based on three sets of rules:

- Ingress Rules
- Forwarding Rules
- Egress Rules

Ingress Rules

Every frame received by the switch is classified to exactly one VLAN. There are two ways in which frames are classified to VLANs:

- Untagged frames are classified to the VLAN associated with the port on which the frame is received (Port-based VLANs)
- Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame

Forwarding Rules

These rules determine the set of ports on the switch through which members of the VLAN can be reached. This is called binding a port to a VLAN. A port may be bound to a VLAN using the following four methods:

- Setting the Port VLAN attribute in the Switch Port Configuration web page. This identifies the VLAN to which all untagged frames received on the port are classified. Note that a port has exactly one Port VLAN. Changing this to a new VLAN removes the port from the old VLAN.
- Setting the VLAN Binding attribute in the Switch Port Configuration web page to Bind to All. This causes the port to be bound to all VLANs known to the switch (now and in the future).
- Setting the VLAN Binding attribute in the Switch Port Configuration web page to Bind to Received. This causes the port to be bound to all VLANs identified by the VLAN tag in IEEE 802.1Q and Multi-Layer tagged frames received on this port. Consequently, ports are bound to those VLANs that actually have members that are reachable through the port.
- Manually creating a VLAN Switch Port via the CLI.

Egress Rules

For a given port/VLAN combination, these rules determine whether frames transmitted from the port on the VLAN are tagged or untagged. This is accomplished by setting the Trunk Mode attribute in the Switch Port Configuration Web page. For example, choosing the IEEE 802.1Q Trunk Mode causes all frames transmitted out of the port to be tagged using the IEEE 802.1Q tag header format. Individual port/VLAN combinations may be changed to cause frames transmitted from the port to be untagged for particular VLANs.

Relationship Between Different Switch Port Parameters

Refer to Table 5-3 the relationship between Port VLAN / Trunk Mode / VLAN Binding parameters can be summarized in the following table using the VLAN Operational Rules.

Table 5-3. Relationship Between Switch Parameters

VLAN Binding	Trunk Mode	Description
Static	Clear	**Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame. **Forwarding:** Only forward frames to the port for the assigned VLAN. **Egress:** All frames transmitted will be sent with no tagging.
Static	802.1Q Multi-layer	**Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame. **Forwarding:** Only forward frames to the port for the assigned VLAN. **Egress:** All frames transmitted out of the port to be tagged using the IEEE 802.1Q/Multi-Layer tag header format. The tagged used will be that assigned to the port.
Bind to All	Clear	***NOT RECOMMENDED*** **Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame. **Forwarding:** All broadcast frames from all VLANs will be forwarded to the port. **Egress:** All frames transmitted will be sent with no tagging.

***Table 5-3. Relationship Between Switch Parameters** continued*

VLAN Binding	Trunk Mode	Description
Bind to All	802.1Q Multi-layer	**Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame. **Note:** For 802.1q mode: if a tagged frame is received, but the VLAN for that tagged frame does not exist on the switch, that frame will placed onto the port VLAN assigned to the port. This may cause unicast and broadcast VLAN traffic from other VLANs to be seen on the port VLAN. To avoid this behavior, you can set the port VLAN into the "discard" VLAN which will drop all untagged frames and tagged frames with unknown VLAN IDs. For Multi-layer and 3Com mode: if a tagged frame is received, but the VLAN for that tagged frame does not exists on the switch, that frame will be dropped. **Forwarding:** All broadcast frames from all VLANs will be forwarded to the port. **Egress:** All frames transmitted out of the port to be tagged using the IEEE 802.1Q/Multi-Layer tag header format. The tagged used will be that of the VLAN in which the frame was received.
Bind to Received	Clear	***NOT RECOMMENDED*** **Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame. **Forwarding:** All broadcast frames from all VLANs learned on the port will be forwarded. **Egress:** All frames transmitted will be sent with no tagging.

***Table 5-3. Relationship Between Switch Parameters** continued*

VLAN Binding	Trunk Mode	Description
Bind to Received	802.1Q Multi-layer	**Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.** **Note:** For 802.1q mode: if a tagged frame is received, but the VLAN for that tagged frame does not exist on the switch, that frame will placed onto the port VLAN assigned to the port. This may cause unicast and broadcast VLAN traffic from other VLANs to be seen on the port VLAN. To avoid this behavior, you can set the port VLAN into the "discard" VLAN which will drop all untagged frames and tagged frames with unknown VLAN IDs. For Multi-layer and 3Com mode: if a tagged frame is received, but the VLAN for that tagged frame does not exists on the switch, that frame will be dropped. **Forwarding:** All broadcast frames from all VLANs learned on the port will be forwarded. **Egress:** All frames transmitted out of the port to be tagged using the IEEE 802.1Q/Multi-Layer tag header format. The tagged used will be that of the VLAN in which the frame was received.
N/A	3Com	**Ingress:** Untagged frames are not allowed (in most cases untagged frames will be dropped). Tagged frames are classified to the VLAN corresponding to the 3Com tag in the corresponding entry of the 3Cm Mapping Table assigned to the port. **Forwarding:** Only forward frames to the port that belongs to the VLANs listed in the 3Com Mapping Table of the port. **Egress:** All frames transmitted out of the port to be tagged using the 3Com tag header format. The tagged used will be that of the VLAN in which the frame was received.

Assigning VLANs to a Port and Associated Issues

There are two ways to assign VLANs to ports on the P550/P880/P882 switch. The first, and recommended way, is to assign the VLAN to a port under the 'Module & Ports / Switch Ports' menu on the web agent. You configure the 'Port VLAN' to the VLAN desired for the individual port (or entire module if configuring that way). Assigning the VLAN via this route will enable the port(s) to receive information for the assigned VLAN and more importantly, this causes all untagged frames arriving on this port to be assigned to the specified VLAN. The port will still assign incoming tagged packets to the VLAN indicated by the tag.

In the current release of software, a non-trunk port only supports a single VLAN per port. Multiple VLANs per port is NOT recommended and can have adverse effects on network performance.

The second way is to assign the VLAN to a port is to use the following CLI command in **Priv/Configure** mode:

```
> set port vlan
```

By selecting the VLAN name, you can bind the selected VLAN to additional ports. When binding VLANs via this route, the port is part of the flooding domain of the selected VLAN. This is an alternative to using the binding types "bind to all" and "bind to receive", that allows you to add a port to a subset of VLANs in the switch. This configuration should only be used under special circumstances and with the assistance of customer support as undesirable results may occur (e.g. destination unknown unicast storms).

See Chapter 4, "Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping", for a description of the parameters that will be displayed when viewing VLAN information via the http management interface.

Although this method of adding VLANs to a port could be thought to support the request for multiple VLANs per port (also referred to as overlapping VLANs), it is NOT recommended on clear ports due to the impact it has on the network. The impact is that destination unknown unicast packets is flooded on the VLAN in which the source host is located. This causes all ports assigned to this VLAN to receive the destination unknown unicast. If enough of these destination unknown unicast packets are being sent it could have a major impact on the network.

The following is an example of this problem.

- All PCs and Servers are connected to P550/P880 10/100TX switch ports
- PC1–VLAN1 (via Module & Ports)–PORT1 ---> P550
- PC2–VLAN2 (via Module & Ports)–PORT2 ---> 10/100BT
- SERVER1-VLAN4 (via Module & Ports)–PORT4 ---‡ PORTS

If you then assign port 1 and port 2 to VLAN4 (via Virtual LANs) and also assign port 4 to VLAN1 and VLAN2 (via Virtual LANs), you could have PC1 and PC2 communicate to SERVER1 across VLANs without any noticeable problems. However, when PC1 transmits a packet to SERVER1, the following occurs:

- The packet is sent to the P550
- The P550 looks in the AFT in VLAN1 for the MAC address of SERVER1 (because this is the actual port van assigned to the port)
- The P550 will be unable to find an entry for the MAC address of SERVER1
- The P550 will flood this packet to all ports assigned to VLAN1 (regardless of how the VLAN was assigned to the port)

***Note:** The only exception to flooding a port is of 'Known Mode' is set to enable on the port

Therefore, if you had many clients/servers on separate VLANs and tried to have them communicate over multiple VLANs using this method, you would flood your network with undesired packets, thus slowing your overall network performance. Currently, the best solution is to use a L3 P550 to route between the VLANs. This would eliminate the broadcast of destination unknown unicast packets.

Configuring Physical Port Parameters on Gigabit Ports

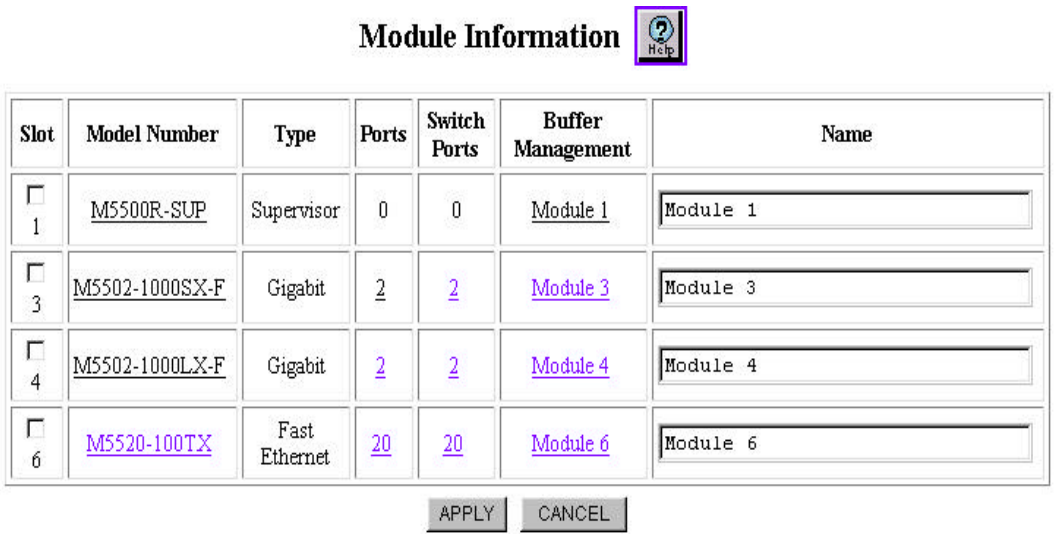
You can configure the physical port parameters on Gigabit ports using either the web agent or the CLI.

Configuring Physical Port Parameters on Gigabit Ports Using the Web Agent

To configure ports on a gigabit module using the web agent:

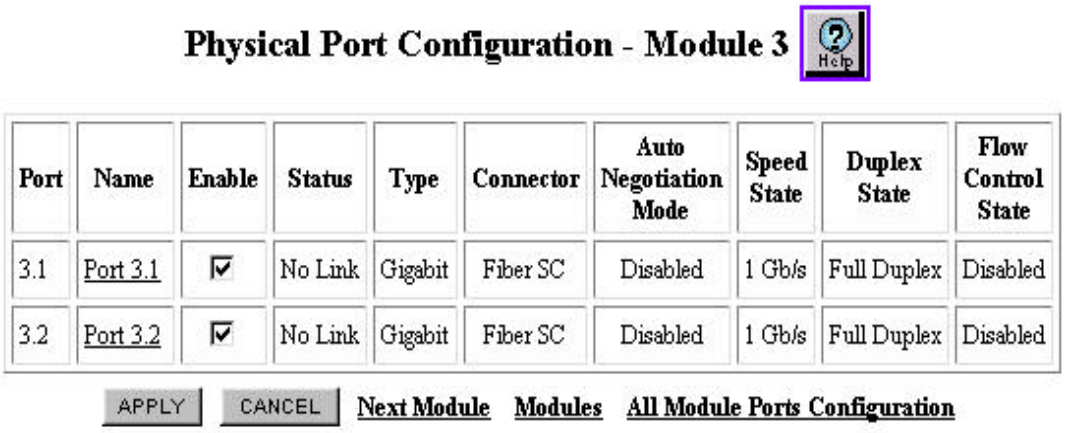
1. Select Configuration from the Modules & Ports group on the web agent window. The Module Information dialog box opens (Figure 5-1).

Figure 5-1. Module Information Dialog Box



2. Select the checkbox in the Slot column for the Gigabit module that you want to configure. The Physical Port Configuration dialog box for that module opens (Figure 5-2).

Figure 5-2. Gigabit Ethernet Module Physical Port Configuration Dialog Box



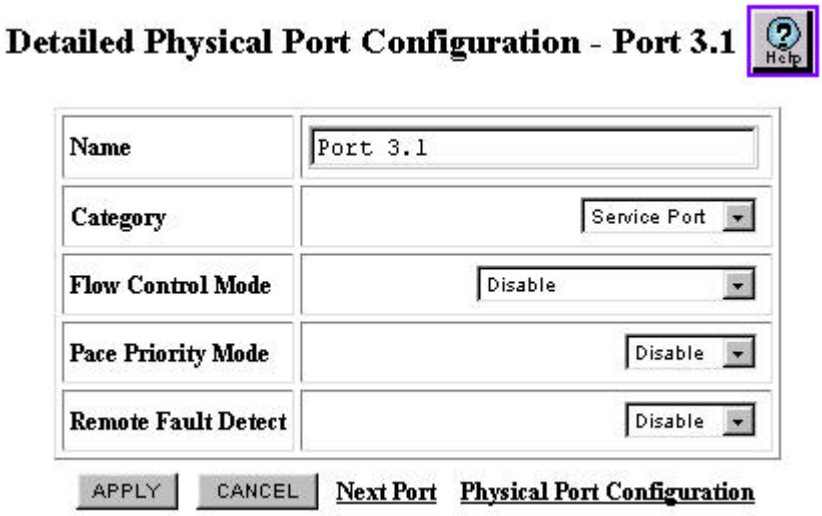
3. Click the checkbox in the Enable column to Enable a port. A checkmark displays.

   ***Note:** If the port is already enabled (checkmark is visible), click on the box to Disable the port (checkmark vanishes).

4. Click APPLY to save your settings, or CANCEL to restore previous settings.

5. Select the port name from the Name field. The Detailed Physical Port Configuration dialog box opens (Figure 5-3).

Figure 5-3. Detailed Port Configuration Window



6. Enter a port name in the Name field.

7. Select one of the following options from the Category field pull-down menu:

User Port - if this is an end-station port

Service Port - if this is a trunk port.

8. Select one of the following an options from the Flow Control Mode field pull-down menu:

Enable – Set flow control to prevent buffer overflows.

Disable – When flow control is causing congestion in other areas of the network.

Enable (Send Only) – Set flow control to prevent buffer overflows on sent traffic.

Enable (Respond Only) – Set flow control to prevent buffer overflows on respond traffic.

9. Select Enable from the Pace Priority Mode field pull down menu to recognize and use 3Com's PACE priority mechanism.

10. Select Enable from the Remote Fault Detect field pull down menu to detect remote link errors.

***Note:** You must set the remote fault detection functionality to enable on both ends of a Cajun to Cajun link in the following cases:

- When two Cajun gigabit ports are connected that do not support auto-negotiation.
- When a Cajun gigabit port that does not support autonegotiation is connected to a Cajun gigabit port that does support autonegotiation. If two gigabit ports that support autonegotiation are connected, you should enable auto-negotiation.

You cannot concurrently enable autonegotiation and remote fault detection. Autonegotiation must be disabled in order to enable remote fault detection. When autonegotiation is enabled, remote fault detection is automatically disabled.

11. Click APPLY to save your changes, or CANCEL to restore previous settings.

Refer to Table 5-4 provides a more detailed description of the Detailed Physical Port dialog box parameters.

Table 5-4. Detailed Physical Port Dialog Box Parameters

Parameter	Definition
Name	A user-assigned name for this port (possibly a drop name or the name of the station or other device connected to the port).
Category	The **User Port** option is intended for use with switch connections to end user nodes. It is intended for use with switch connections to servers or other switches. The **Service Port** allows the switch to generate both log messages and alarm messages (traps). The User Port only generates log messages. This prevents your network management station from being overwhelmed by port up/down messages that result from users turning workstations on and off.

Table 5-4. Detailed Physical Port Dialog Box Parameters continued

Parameter	Definition
Flow Control Mode	Setting this field determines if the IEEE 802.3z pause control is to be used on this port. The pause mechanism allows the port to stop a sending station from sending more packets if the receiving port's buffers are full. This helps prevent lost or dropped packets. This feature is recommended for use primarily on end station connections. Using this feature on trunk ports can cause unnecessary congestion on the network.
PACE Priority Mode	Determines if the port detects 3Com's copyrighted PACE format as packets pass through the port. PACE allows a packet's priority (higher priority packets move through the switch faster) to be set at the adapter.
Remote Fault Detect	Proprietary mechanism to detect remote link errors on Cajun gigabit ports. The default value is Disabled. The remote fault detection functionality should be enabled (on both ends of a Cajun to Cajun link) in two cases: • When two Cajun gigabit ports are connected that do not support auto-negotiation. • When a Cajun gigabit port that does not support auto-negotiation is connected to a Cajun gigabit port that does support auto-negotiation.

Configuring Physical Port Parameters on Gigabit Ports Using the CLI

To configure ports on a gigabit module using the CLI, enter the following command from Priv mode:

```
cajun# port set <options>
```

Refer to the *Cajun P550/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Configuring Physical Port Parameters on Fast Ethernet Ports

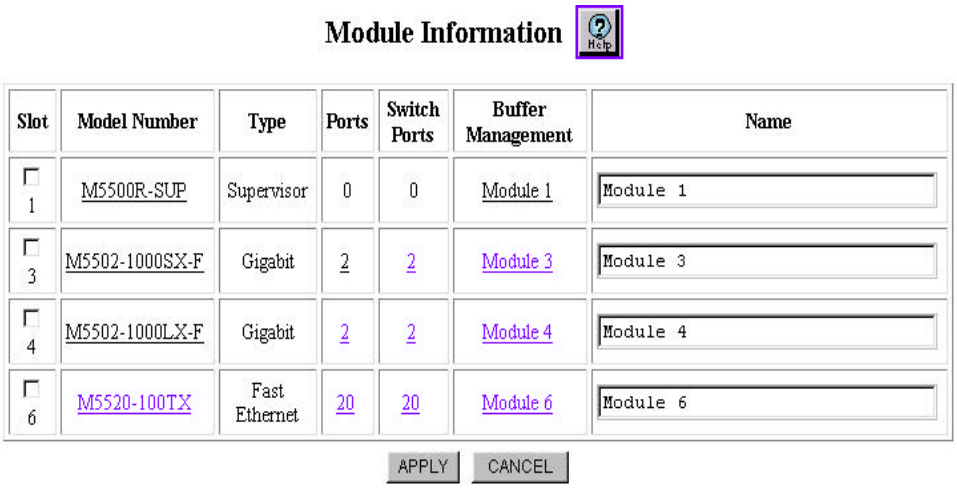
You can configure ports on a Fast Ethernet module using either the web agent or CLI commands.

Configuring Physical Port Parameters using the Web Agent

To configure ports on a Fast Ethernet module using the web agent:

1. Select Configuration from Modules & Ports group on the web agent window. The Module Information dialog box opens (Figure 5-4).

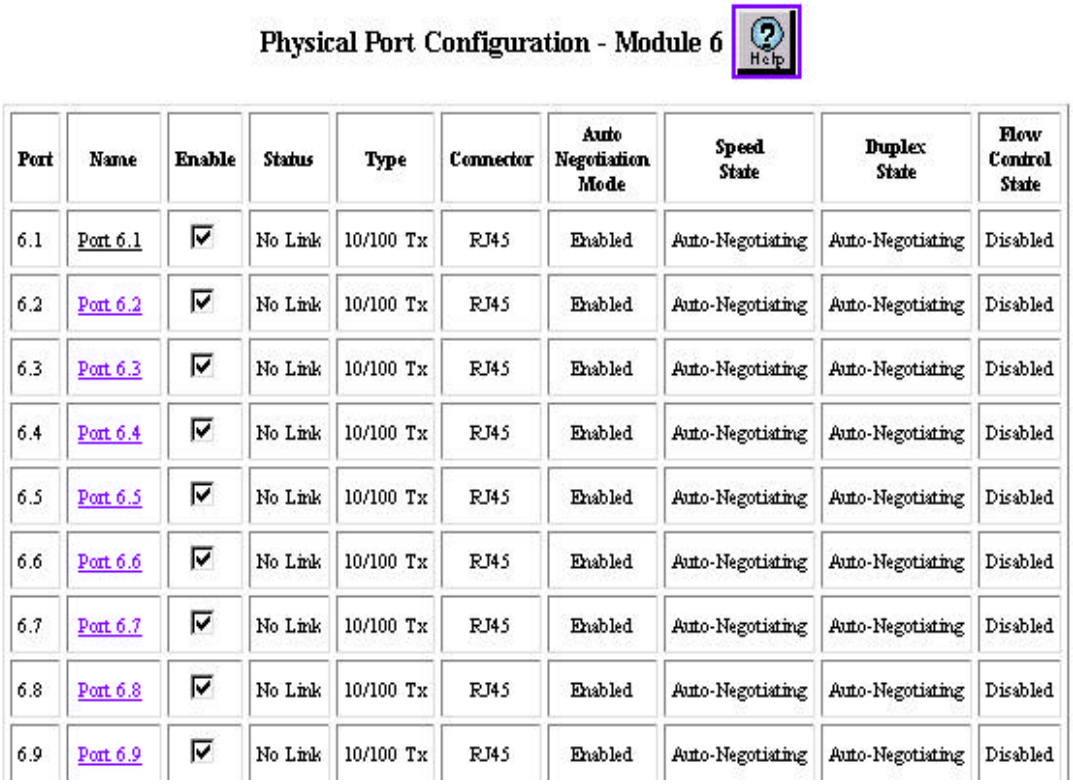
Figure 5-4. Module Information Dialog Box



2. Select the checkbox in the Slot column next to the Fast Ethernet module on which you want configure the physical port parameters.

3. Select the number in the Ports column for the Fast Ethernet module that you want to configure. The Physical Port Configuration window opens (Figure 5-5).

Figure 5-5. Physical Port Configuration Window for the Fast Ethernet Module installed in Slot 6 (partial view)

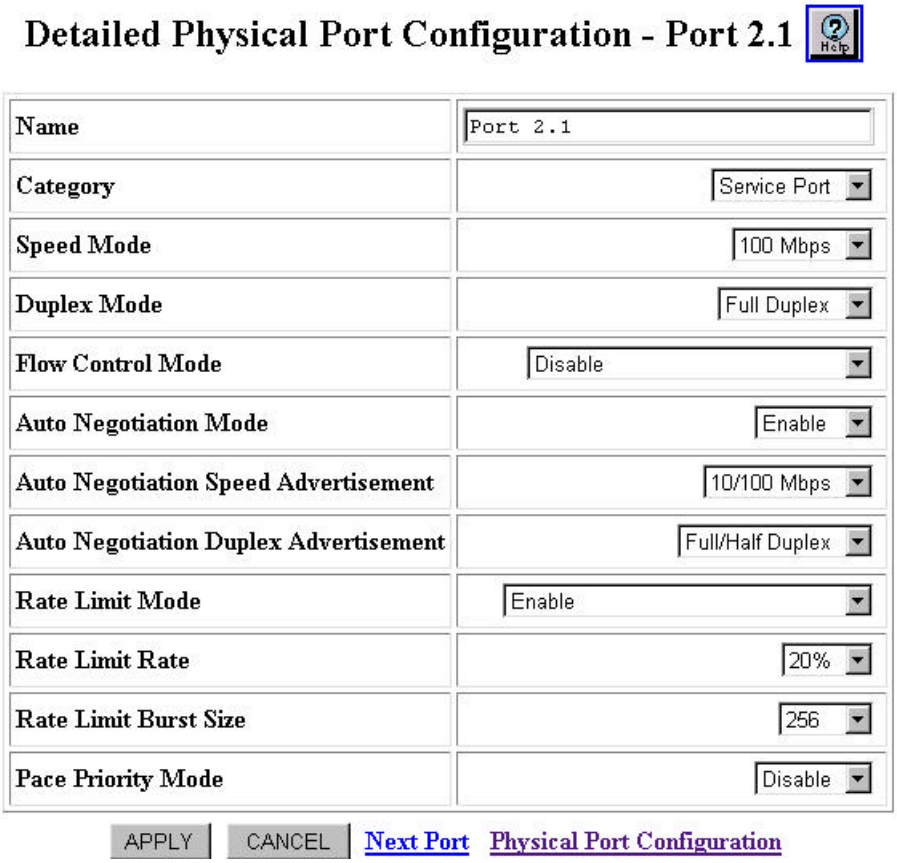


Physical Port Configuration - Module 6

Port	Name	Enable	Status	Type	Connector	Auto Negotiation Mode	Speed State	Duplex State	Flow Control State
6.1	Port 6.1	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.2	Port 6.2	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.3	Port 6.3	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.4	Port 6.4	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.5	Port 6.5	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.6	Port 6.6	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.7	Port 6.7	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.8	Port 6.8	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled
6.9	Port 6.9	☑	No Link	10/100 Tx	RJ45	Enabled	Auto-Negotiating	Auto-Negotiating	Disabled

4. Click the checkbox in the Enable column to enable the port you want to configure. A check mark displays indicating the port is enabled.
5. Click APPLY located at the bottom of the dialog box to save your settings, or CANCEL to restore previous settings.
6. Select a port name from the Name field (for example, Port 6.1). The Detailed Physical Port Configuration dialog box for that port opens (Figure 5-6).

Figure 5-6. Detailed Physical Port Configuration Window



7. Enter a port name in the Name field.

8. Select one of the following from the Category field pull-down menu:

   — User Port if this is an end-station port

   — Service Port if this is a trunk port.

9. Select a speed (10 Mb/s or 100 Mb/s) from the Speed Mode field pull down menu, If you want to set the port speed manually. If want the port to autonegotiate, you can ignore this field.

   ***Note:** This feature is only available for 10/100 TX modules.

10. Select a duplex mode (half-duplex or full-duplex) from the Duplex Mode field pull-down menu if you want to manually set the port's duplex mode. You do not have to select a duplex mode if you set the port to autonegotiate.

11. Select one of the following from the Flow Control Mode field pull down men:

Enable – Sets flow control to prevent buffer overflows.

Disable – Disables flow control when it is causing congestion in other areas of the network.

Enable (with Aggressive Backoff) – Limits the size of flow control burst on TX and FX ports.

12. Select Enable from the Auto Negotiation Mode field pull down menu to enable Auto Negotiation.

***Note:** This feature is only available for 10/100 TX modules.

Auto Negotiation works best when the port or device on the other end of the connection is also set to Auto Negotiation. If you are having problems with Auto Negotiating connections, manually set the modes using the CLI. See the *Cajun P550/P200 Command Line Interface Reference Guide* for more information.

13. Select a speed from the Auto Negotiation Speed Advertisement pull- down menu. The options are 10Mbps, 100Mbps. or 10/100Mbps.

14. Select a duplex option from the Autonegotiation Duplex Advertisement field pull-down menu. The options are Full/Half Duplex and Half Duplex).

***Note:** The Speed and Duplex features are only available for 10/100 TX modules.

The switch sends the Speed and Duplex advertisement values to the device on the other end of the connection at the start of the auto-negotiating process. In general, the defaults are best, but there may be situations when you want to fix one setting, but allow the other setting to auto-negotiate.

15. Select one of the following from the Rate Limit Mode pull-down menu:

Enable – If you want this port to limit the number of unknown unicast and multicast (flooded) packets it tries to forward

Disable – If you do not want this port to limit the number of unknown unicast and multicast packets it tried to forward

Enable (include Known Multicasts) – If you want to optionally include known multicast packets in this percentage to further decrease the possibility of the port's output buffer that is being overwhelmed.

16. Select the percentage of a port's traffic that can be unknown unicast and broadcast packets from the Rate Limit Rate field pull-down menu.

***Note:** Set this value lower if the port is having overflow problems.

17. Open the Rate Limit Burst Size pull down menu (Figure 5-18).

18. Select a packet limit for the number of packets allowed in a single burst. The values are 1 to 2048.

***Note:** Set this value lower than 1024 (the output buffer's capacity) for Fast Ethernet ports. Also set this value lower if the port is experiencing overflow problems.

19. Select Enable from the Pace Priority Mode pull-down menu if you want this port to recognize and use 3Com's PACE priority mechanism.

20. Click APPLY to save your changes, or CANCEL to restore previous settings.

Refer to Table 5-5 describes in detail the Fast Ethernet port parameters:

Table 5-5. Fast Ethernet (10/100) Port Parameters

Parameter	Definition
Name	Enter a name for this port (possibly a drop name or the name of the station or other device connected to the port).
Category	Select either User Port or Service Port. • The **User Port** is intended for use with switch connections to end user nodes. • The **Service Port** is intended for use with switch connections to servers or other switches. The Service Port allows the switch to generate both *log messages* and *alarm messages* (traps). The User Port only generates log messages, preventing your network management station from being overwhelmed by port up/down messages that result from users turning workstations on and off.
Speed Mode	Select the speed of the port manually (to either 10 or 100 Mb/s). **If auto-negotiation is enabled, this setting is ignored.**
Duplex Mode	Select the port duplex mode (half- or full-duplex). **If auto-negotiation is enabled, this setting is ignored.**
Flow Control Mode	Determines if flow control is used on this port. For half-duplex links, active backpressure jams the sending Ethernet channel until the port's buffers can receive more packets. This prevents lost or dropped packets. For full-duplex links, IEEE 802.3z pause control allows the port to stop a sending station from sending more packets if the receiving port's buffers are full. For TX and FX ports, there is an additional option for Enable with Aggressive Backoff. This option limits the size of the bursts. Flow Control is recommended for use primarily on end-station connections. Using this flow control on trunk ports can cause unnecessary congestion on the network.

Table 5-5. Fast Ethernet (10/100) Port Parameters continued

Parameter	Definition
Auto Negotiation Mode	Select the port to auto-negotiate a speed and duplex mode. Auto-negotiate works best when the connection on the other end of the link is set to auto-negotiate as well. If you set a port to auto-negotiate, and the connection is not successful, set the port speed and duplex mode manually.
Auto Negotiation Speed/Duplex Advertisement	Determines what information the port advertises when it starts auto-negotiating. In most cases, **10/100** and **Half/Full** are the best settings, but there may be cases when you want to auto-negotiate one parameter, while keeping the other fixed.
Rate Limit Mode	Prevents the switch from overwhelming the output buffer on lower-speed ports by placing a threshold on the percentage of port traffic that can be flooded packets (unknown unicasts and multicasts). You can also optionally include known multicast packets in this percentage to further decrease the possibility of the port's output buffer that is being overwhelmed.
Rate Limit Rate	Determines the percentage of a port's forwarded traffic that can be unknown unicast and multicast (flooded). Lower this value if the port has overflow problems.
Rate Limit Burst Size	Enter a value for the limit of packets allowed in a single burst. Accepted values are 1 to 2048. For Fast Ethernet ports, set this value lower than 1024 (output buffer capacity). Lower this value if the port has overflow problems.
Port PACE Priority	Select Enable to allow the port to detect 3Com's proprietary PACE format as packets pass through the port. PACE allows a packet's priority (higher priority packets move through the switch before lower priority packets) to be set at the adapter.

Configuring Physical Port Parameters on Fast Ethernet Ports Using the CLI

To configure ports on a Fast Ethernet module using the CLI, enter the following command from Priv mode:

```
cajun# port set <options>
```

Refer to the *Cajun P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

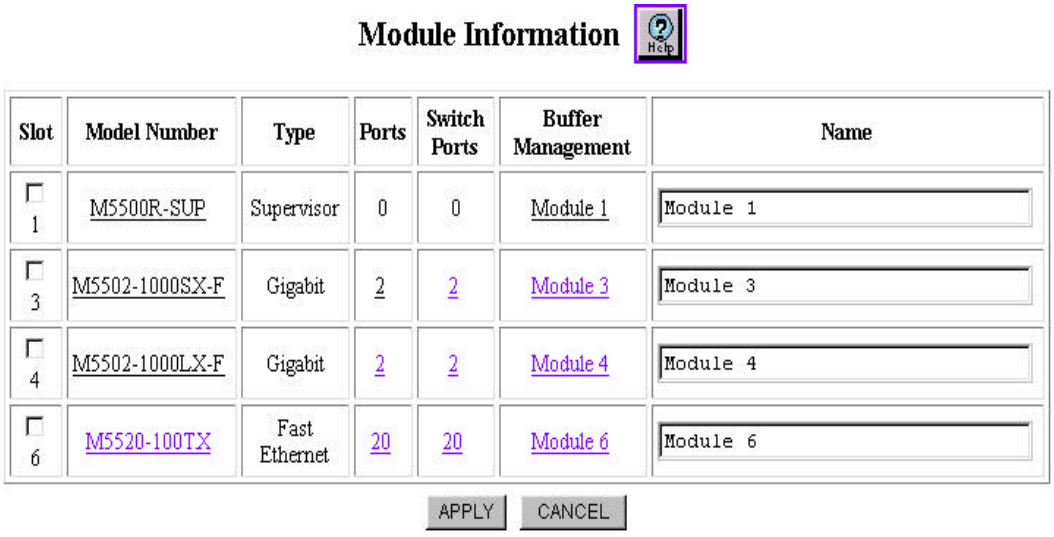
Using the All Ports Configuration Window

You can apply the same parameter settings on all of a module's ports using the All Ports Configuration dialog box.

To configure all ports on a module:

1. Select Configuration from the Modules & Ports group on the web agent window. The Module Information dialogue box opens (Figure 5-7).

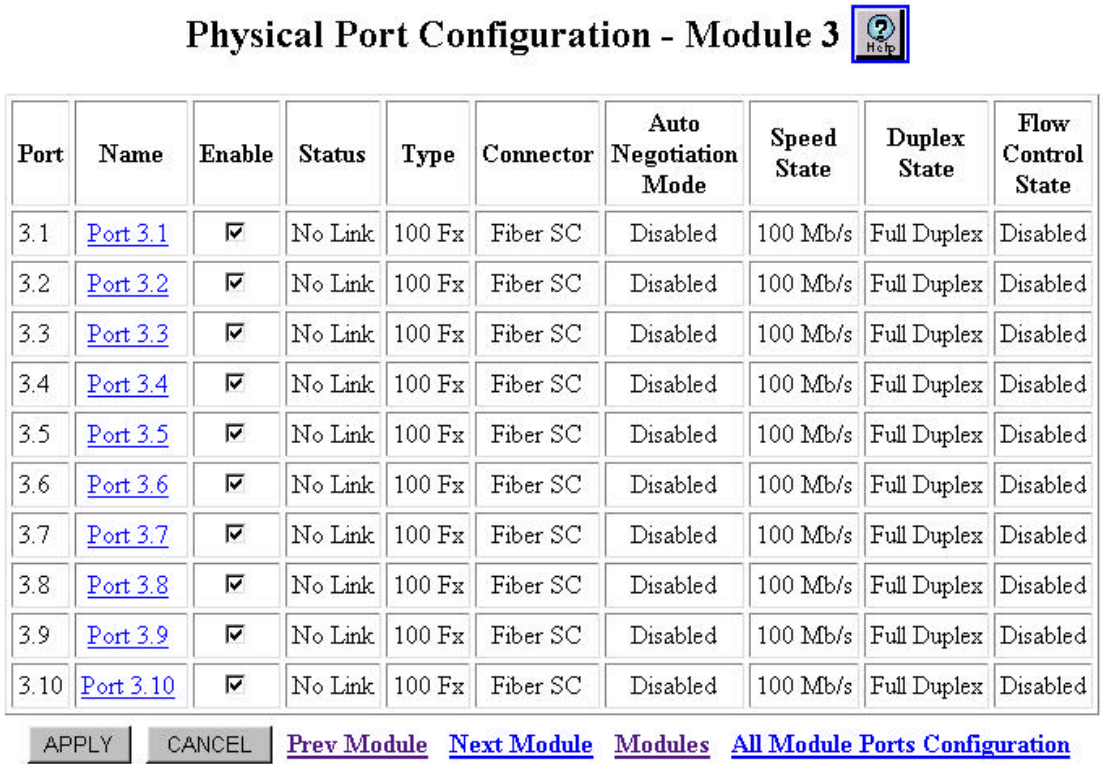
Figure 5-7. Module Information Dialog Box



2. Select the checkbox in the Slot column for the module (for example, slot 3) that you want to configure.

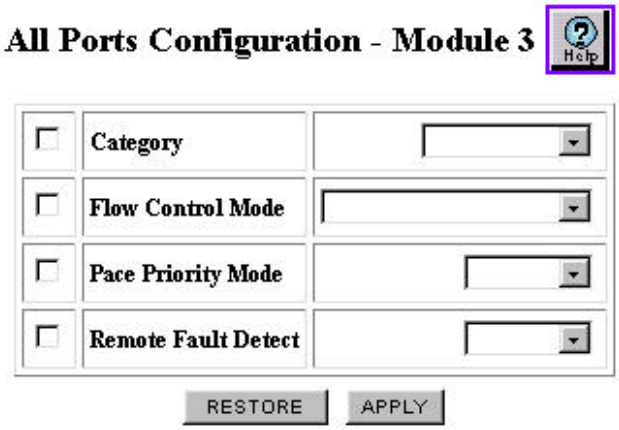
3. Select the port number from the Ports column for that module. The Physical Port Configuration dialog box for that module opens (Figure 5-8).

Figure 5-8. Physical Port Configuration Dialog Box


Physical Port Configuration - Module 3
Help
Port
Name
Enable
Status
Type
Connector
Auto Negotiation Mode
Speed State
Duplex State
Flow Control State
3.1 Port 3.1 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.2 Port 3.2 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.3 Port 3.3 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.4 Port 3.4 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.5 Port 3.5 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.6 Port 3.6 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.7 Port 3.7 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.8 Port 3.8 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.9 Port 3.9 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
3.10 Port 3.10 No Link 100 Fx Fiber SC Disabled 100 Mb/s Full Duplex Disabled
APPLY
CANCEL
Prev Module
Next Module
Modules
All Module Ports Configuration

4. Select All Module Ports Configuration. The All Ports Configuration dialog box opens (Figure 5-9).

Figure 5-9. All Module Ports Configuration Dialog Box



5. Refer to the "Configuring Physical Port Parameters on Gigabit Ports Using the Web Agent" and/or "Configuring Physical Port Parameters on Gigabit Ports Using the CLI" sections earlier in this chapter and configure the port parameters as described in those chapters.

6. Click APPLY to save your changes, or Restore to restore previous settings.

Viewing Switch Port Parameters

You can view switch port parameters through either the web agent and the CLI.

Viewing Switch Port Parameters Using the Web Agent

To view switch port parameters using the web agent:

1. Select Configuration from the Modules & Ports group of the web agent window. The Module Information dialog box opens (Figure 5-7).

2. Select the checkbox in the Slot column for the gigabit module that you want to configure.

3. Select the switch ports for that module from the Switch Ports column. The Switch Ports dialog box opens (Figure 5-10).

Figure 5-10. Switch Ports Dialog Box

Switch Ports Help

Module Number 3

Links	Port	Name	Port VLAN	VLAN Classification	Trunk Mode	Hunt Group	STAP Mode	MAC Address
Port Statistics	3.1	Port 3.1	Default	Port Based	CLEAR	[None]	Enable	02-e0-3b-02-41-68
Port Statistics	3.2	Port 3.2	Default	Port Based	CLEAR	[None]	Enable	02-e0-3b-02-41-69

Next Module **Modules** All Module Switch Ports Configuration

4. Refer to Table 5-3 for more information about the Switch Port dialog box parameters:

Table 5-6. Switch Port Parameters

Parameter	Definition
Links	Opens associated windows.
Port	Displays the port associated with the selected module.
Name	Displays the port name and opens the Switch Port Configuration window for the selected module.
Port VLAN	Displays the port VLAN for the selected module.
VLAN Classification	Displays the port VLAN classification for the selected module.
Trunk Mode	Displays the port's trunk mode for the selected module.
Hunt Group	Displays the hunt group of which the port is a member for the selected module.
STAP Mode	Displays whether the spanning tree algorithm protocol is enabled or disabled for the selected module.
MAC Address	Displays the port's MAC address for the selected module.

5. Select one of the following items listed at the bottom of the screen for more information about the switch ports:
   - **Next/Previous Module** – Displays the next or previous module's switch port parameters.
   - **Modules** – Returns you to the Module Information window.
   - **All Module Switch Ports Configuration** – Opens the Switch Port Configuration All Ports window and configures all ports for the selected module.

Viewing Switch Port Parameters Using the CLI

To view switch port parameters using the CLI, enter the following command from Priv mode:

```
> show port [{<mod-num>|<mod-swport-range>}
[...,{<mod-num>|<mod-swport-range>}]]
```

Refer to the *Cajun P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Configuring Switch Port Parameters

You can configure how each switch port performs its switching functions (for example, VLAN parameters, hunt group assignments, trunk mode, and frame tag scheme) through the switch port parameters.

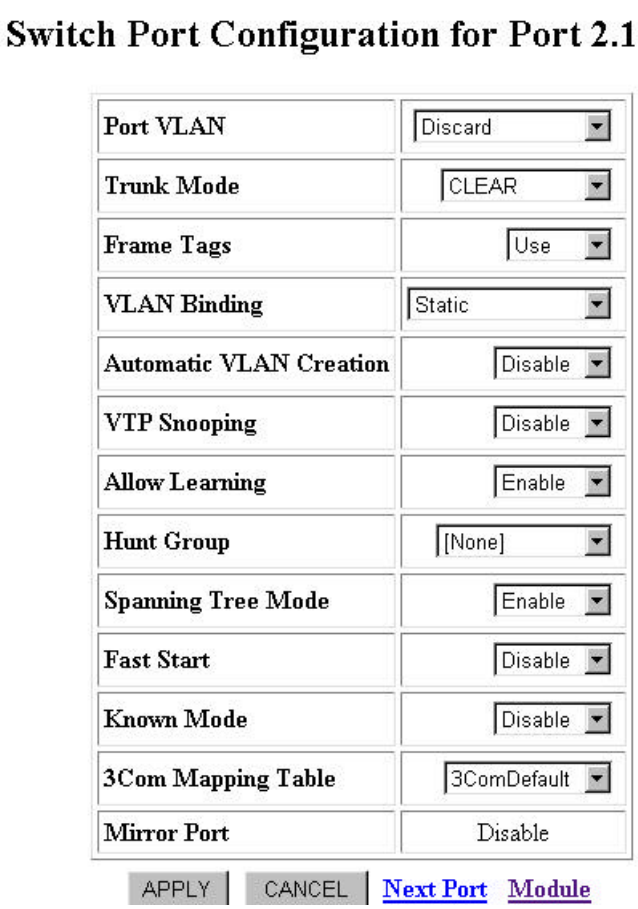
You can configure switch port parameters using either the web agent or the CLI.

Configuring Switch Port Parameters Using the Web Agent

To configure switch port parameters using the web agent:

1. Select Configuration from the Modules & Ports group on the web agent window. The Module Information dialog box opens (Figure 5-7).
2. Select the checkbox in the Slot column for the module on which you want to configure the switch ports.
3. Select the switch ports for that module from the Switch Ports column. The Switch Ports dialog box opens (Figure 5-10).
4. Select a port name from the Name column. The Switch Port Configuration dialog box opens (Figure 5-11).

Figure 5-11. Switch Port Configuration Dialog Box



Refer toTable 5-7 for a description of the Switch Port Configuration dialog box parameters.

Table 5-7. Switch Port Configuration Parameters

Parameter	Definition
Port VLAN	Specifies the VLAN assignment for this port.
Trunk Mode	Select the appropriate VLAN trunking format to make the port a trunk, or Clear (default) if you do not want the port to be a trunk. The trunk formats are IEEE 802.1Q, Multi-Layer, and 3Com.
Frame Tags	Select Ignore if you do not want to use received Frame VLAN tags. Use is the default. **Note:** If you select ignore, the received frames are bound to the port's default VLAN.
VLAN Binding	Select the port's outgoing VLAN binding type. Refer to Table 5-8 for more information on VLAN binding options.

Table 5-7. Switch Port Configuration Parameters continued

Parameter	Definition
Automatic VLAN Creation	Select Enable to automatically create a VLAN each time the port receives a frame from an unknown VLAN. Disable is the default.
VTP Snooping	Select Enable to allow VTP Snooping on this port. Disable is the default.
Allow Learning	Select Disable to keep the port from learning new MAC addresses and forward them to the CPU to be added to the VLANs AFT. Enable is the default. **Note:** If a MAC address is moved to a different VLAN, it will co-exist in AFTs, one entry for each VLAN (This is a benefit of having multiple forwarding databases).
Hunt Group	Select a hunt group for which this port will be a member. None is the default.
Spanning Tree Mode	Select Disable to remove STP on this port. Enable is the default.
Fast Start	Select Enable for fast start on this port. Disable is the default.
Known Mode	Specifies whether or not the port will broadcast traffic with an unknown destination in the address forwarding table (e.g., destination unknown unicast packets). Disable allows broadcast traffic with an unknown destination to be transmitted over the port (default). Enable allows the port to only forward frames with known destinations in the address forwarding table.
3Com Mapping Table	Select how incoming tagged frames from 3Com equipment are mapped to Lucent VLANs. The default value is 3ComDefault.
Mirror Port	Displays the status of the mirror port (enabled or disabled). This is a Fast Ethernet only option.

Configuring Switch Ports Using the CLI

To configure switch ports using the CLi, enter the following command from **Configure** mode:

```
> (configure)# set port <options>
```

Refer to the *Cajun P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Configuring Port VLAN Parameters

You can set the parameters on a port VLAN to determine how traffic is flooded to VLANs when tagged and untagged packets are received on the port.

*** Notes:** See the examples later in this section for recommendations on how to set particular trunk port connections.

Refer to VLAN Operation, in Chapter 11, for more information on creating VLANs.

Refer to *"Viewing Switch Port Parameters"*, earlier in this chapter, for information about accessing the Switch Port window.

You can configure port VLAN parameters using either the web agent or the CLI.

Configuring Port VLAN Parameters Using the Web Agent

To configure port VLAN parameters using the web agent:

*** Note:** This procedure begins at the Switch Port Configuration dialog box. Refer to "Configuring Switch Port Parameters Using the Web Agent", steps 1 through 4.

1. Select Default from the Port VLAN field pull-down menu on the Switch Configuration dialog box. This causes all untagged frames arriving on this port to be assigned to the specified VLAN. The port will still assign incoming tagged packets to the VLAN indicated by the tag.

2. Select an option from the Trunk Mode field pull-down menu. The options are Clear (default), IEE 802.1Q, Multi-layer, and 3Com. Refer to Table 5-7 for an explanation of these options.

3. Select an option from the Frame Tags field pull-down menu. The options are Use (default) and Ignore. Refer to Table 5-7 for an explanation of these options.

4. Select an option from the VLAN Binding field pull-down menu. The options are Static (default), Bind-to-All, and Bind-to-Receive. Refer to Table 5-8 for an explanation of these options.

5. Select Enable from the Automatic VLAN Creation field pull-down menu. This automatically creates a VLAN each time the port receives a frame from an unknown VLAN.

   ***Note:** This feature does not create entries in 3Com Mapping Tables. Refer to Creating 3Com Mapping Tables, in Chapter 11, for more information.

6. Click APPLY to save your changes, or CANCEL to restore previous settings.

Table 5-5 describes the VLAN Binding field pull-down menu options.

Table 5-8. VLAN Binding Field Pull-Down Menu Options

Option	Definition
Static	Assigns VLAN membership manually, using the VLAN Switch Ports page described in "*Creating and Implementing VLANs*", in Chapter 11.
Bind to All	Binds this port to all VLANs known to the switch. This is an appropriate mode for switch-to-switch connections. **Note:** When a tagged IEEE 802.1Q packet arrives on a port that is set to bind to all and the VLAN does not exist on the switch, the packet is forwarded on to the VLAN assigned to the port default VLAN for that port. To prevent unintended forwarding of unknown VLAN traffic to the port's default VLAN, configure the port default VLAN to Discard. The automatic VLAN creation feature will not work if the port's default VLAN is the discard VLAN, because the switch does not learn for this VLAN. if you use 3Com Mapping Tables, this setting is ignored.
Bind to Received	Binds this port to any VLAN it receives traffic from. **Note:** If Automatic VLAN Creation is enabled, the port binds to previously unknown VLANs and a VLAN entry is added to the switch VLAN table. If Automatic VLAN Creation is disabled, the port does not bind to any VLAN unknown to the switch.

Configuring Port VLAN Parameters Using the CLI

To configure port VLAN parameters using the CLI, enter the following command from **Configure** mode:

```
Cajun(configure)# set port vlan <options>
```

Refer to the *Cajun P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Configuring Non-VLAN Switch Port Parameters

You can configure non-VLAN switch port parameters using either the web agent or the CLI.

Configuring Non-VLAN Switch Port Parameters Using the Web Agent

To configure Non-VLAN switch port parameters using the web agent:

*** Note:** This procedure begins at the Switch Port Configuration dialog box. Refer to "Configuring Switch Port Parameters Using the Web Agent", steps 1 through 4.

1. Select Disable from the Allow Learning field pull-down menu. This prevents the port from learning new MAC addresses. This feature can be useful for security.

   ***Note:** If you want to allow a port to learn new addresses, reselect Enable. For example, you can set this parameter to Disable, then add a static MAC address entry for this port.

   If you do not select Disable before you add a static MAC address, Unicast flooding can result.

2. Select a Hunt group from the Hunt Group field pull-down menu. Refer to Chapter 4, Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping for more information on hunt groups.

3. Select Disable from the Spanning Tree field pull-down menu to keep STP from running on this port. Reselect Enable to run STP on this port.

4. Select Enable from the Fast Start field pull-down menu to allow Fast Start mode ports to begin forwarding traffic without waiting for STP negotiation to complete. Fast start eliminates the listening and learning waiting times. Ports immediately enter the forward state. Reselect Disable to prevent traffic from being forwarded.

5. Select Enable from the Known Mode field pull-down menu to suppress any packets that have unknown unicast destination addresses and are flooded to this port.

   For example, if a known end-station or file server is connected to the port, there's no need to flood unknown unicasts to that port. You must manually enter a static MAC address for the station actually attached to the port. Reselect Disable to prevent the suppressing of packets.

6. Select 3Com Default from the 3Com Mapping Table field pull-down menu to specify how incoming tagged frames from 3Com equipment are mapped to Lucent VLANs. Refer to "Creating 3Com Mapping Tables", in Chapter 4 for more information.

7. Click APPLY to save your changes, or CANCEL to restore previous settings.

Refer to Table 5-9 through Table 5-11 for examples of the recommended switch port settings for each connection type.

*** Note:** Do not enable Automatic VLAN Creation and VTP Snooping at the same time.

Table 5-9. Example 1. Trunk to Cisco Catalyst 5000™

Parameter	Recommended Setting
Port VLAN	**Default** - Causes untagged packets to be assigned to the default VLAN.
Trunk Mode	**Multi-layer** - Causes the port to send frames using the multi-layer format.
VLAN Binding	**Bind to All** - Binds the port to all VLANs known to the switch.
Automatic VLAN Creation	**Enable (Disable if using VTP Snooping)** - Causes the switch to learn new VLAN IDs that arrive at the port, and then bind the port to these VLANs.
VTP Snooping	**Enable** - Causes the switch to update its VLANs as they are created, deleted, or changed on the Catalyst.

Table 5-10. Example 2. Trunk to 3Com SuperStack™

Parameter	Recommended Setting
Port VLAN	**Default** - This parameter is ignored when using 3Com VLANs.
Trunk Mode	**3Com** - Allows the switch to read the incoming VLAN tags.

Table 5-10. Example 2. Trunk to 3Com SuperStack™ continued

Parameter	Recommended Setting
VLAN Binding	**Static** - This parameter is ignored when using 3Com VLANs.
Automatic VLAN Creation	**Disable** - This parameter is ignored when using 3Com VLANs.

Table 5-11. Example 3. Trunk to Bay Networks System 5000™

Parameter	Recommended Setting
Port VLAN	**Default** - Causes untagged packets to be assigned to the default VLAN.
Trunk Mode	**IEEE-802.1Q** - Causes the port to send frames using the IEEE-802.1Q format. This assumes that you have configured the Bay Networks switch to use IEEE-802.1Q VLAN tagging as well.
VLAN Binding	**Bind to All** - Binds the port to all VLANs known to the switch.
Automatic VLAN Creation	**Enable** - Causes the switch to learn new VLAN IDs that arrive at the port, and then binds the port to these VLANs.

Configuring Non-VLAN Switch Port Parameters Using the CLI

To configure Non-VLAN switch port parameters using the CLI, enter the following command from Priv mode:

```
> vlan create <options>
```

Refer to the *Cajun P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Configuring Fast Start Mode

Fast Start mode causes ports to begin forwarding traffic without waiting for the spanning tree negotiation to complete. You may want to set a port to Fast Start mode in the following examples:

- End-station ports that do not need to participate in the full spanning tree negotiation
- Loop-free topologies that do not need spanning tree protocol to resolve redundant connections
- Endstations that require immediate forwarding of traffic in order to receive configuration information, such as IPX clients or DHCP clients.

You can configure Fast Start mode using either the web agent or the CLI.

Configuring Fast Start Mode Using the Web Agent

To enable Fast Start mode for ports on a module associated with a selected bridge using the web agent:

1. Select Configuration from the Modules & Ports group on the web agent window. The Module Information window opens (Figure 5-12).

Figure 5-12. Module Information Window

Module Information

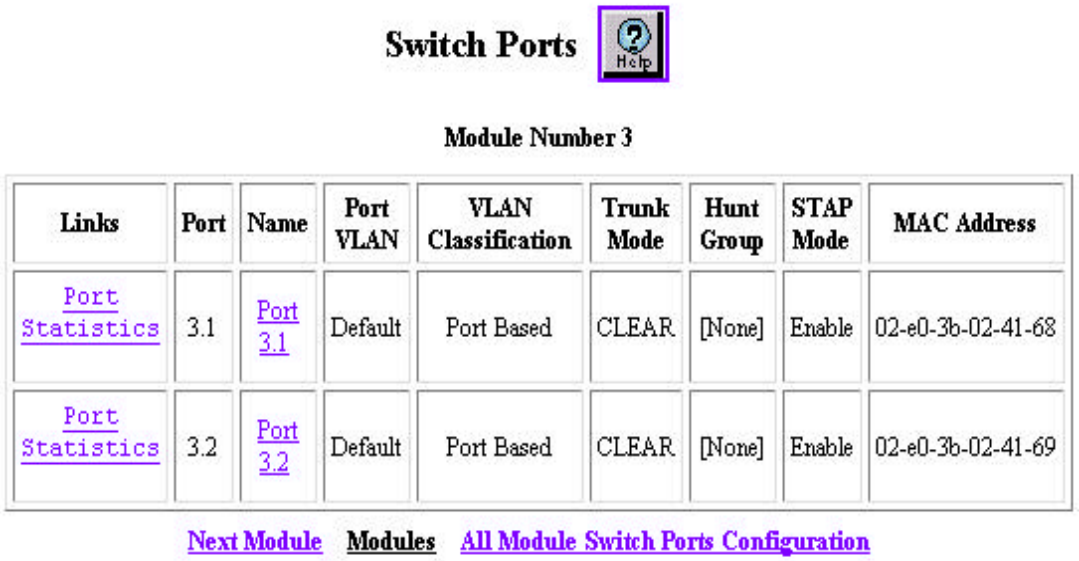
Slot	Model Number	Type	Ports	Switch Ports	Buffer Management	Name
1	M5500R-SUP	Supervisor	0	0	Module 1	Module 1
3	M5502-1000SX-F	Gigabit	2	2	Module 3	Module 3
4	M5502-1000LX-F	Gigabit	2	2	Module 4	Module 4
6	M5520-100TX	Fast Ethernet	20	20	Module 6	Module 6

APPLY CANCEL

2. Select the checkbox in the Slot column next to the Fast Ethernet module on which you want to enable Fast Start mode.

3. Select the switch port number listed for that module from the Switch Ports column. The Switch Ports dialog box opens (Figure 5-13).

Figure 5-13. Switch Ports Dialog Box



a. Select the port name for the selected module in the Name column if you want to set fast mode on individual ports. The Switch Port Configuration window for that module opens.

b. Select All Module Switch Port Configuration if you want to set fast mode on all ports on a module. The Switch Port Configuration on All Ports window for that module opens.

4. Select Enable from the Fast Start field pull-down menu to allow Fast Start mode on the selected module ports.

5. Click APPLY to save your changes, or CANCEL to clear your selection.

Configuring Fast Start Mode Using the CLI

To configure Fast Start mode for ports on a module associated with a selected bridge using the CLI, enter the following command from Configure mode:

```
> (configure)# set port fast-start <options>
```

Refer to the *Cajun P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

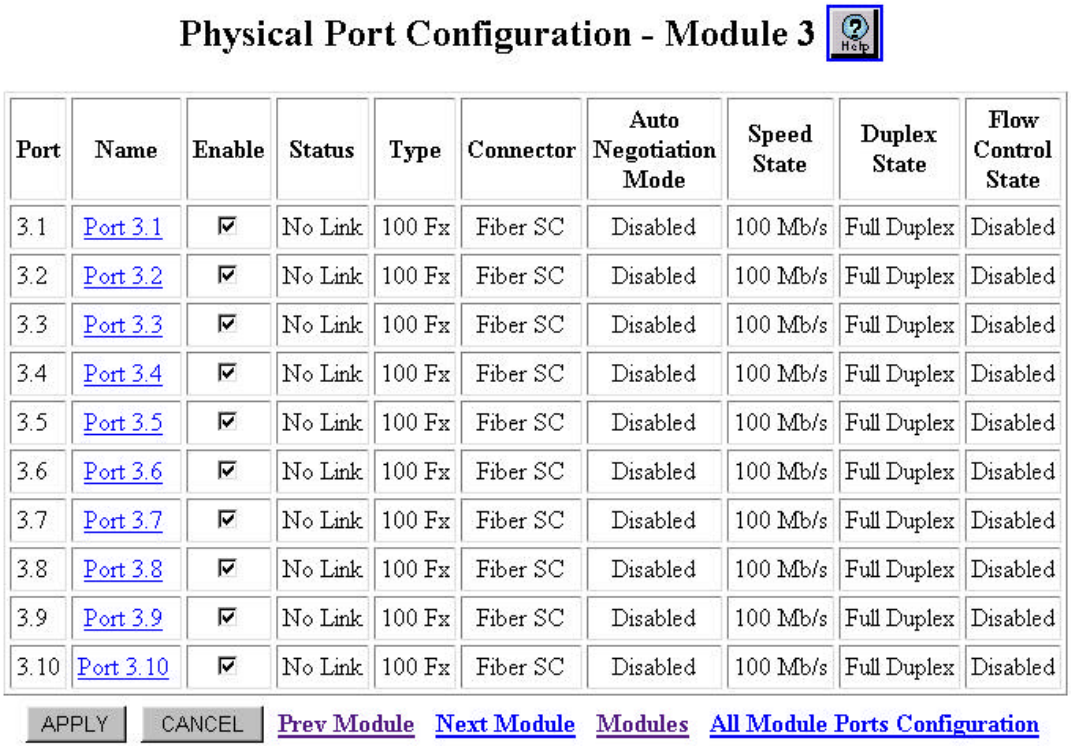
Using the All Module Ports Configuration Window

The All Ports Configuration window allows you to apply the same parameter settings to all switch ports in a module using a single command.

To set all switch ports in a module using a single command:

1. Select Configuration from the Modules & Ports group on the web agent window. The Module Information dialog box opens (Figure 5-12).
2. Select the checkbox in the Slot column next to the module on which you want to configure all of its ports.
3. Select the number in the Ports column for that module. The Physical Port Configuration dialog box for that module opens (Figure 5-14).

Figure 5-14. Physical Port Configuration Dialog Box



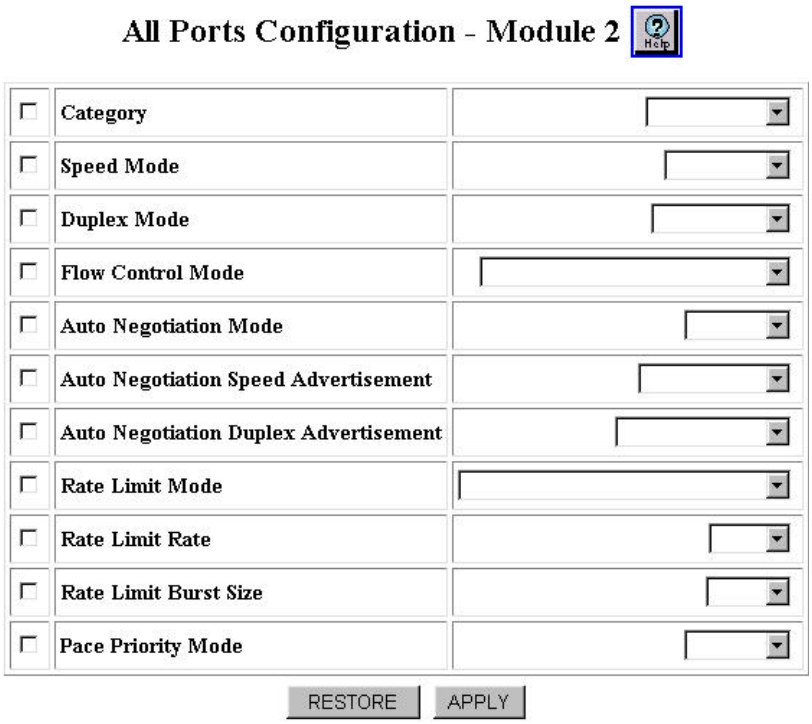
Physical Port Configuration - Module 3

Port	Name	Enable	Status	Type	Connector	Auto Negotiation Mode	Speed State	Duplex State	Flow Control State
3.1	Port 3.1	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.2	Port 3.2	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.3	Port 3.3	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.4	Port 3.4	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.5	Port 3.5	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.6	Port 3.6	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.7	Port 3.7	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.8	Port 3.8	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.9	Port 3.9	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled
3.10	Port 3.10	☑	No Link	100 Fx	Fiber SC	Disabled	100 Mb/s	Full Duplex	Disabled

APPLY CANCEL Prev Module Next Module Modules All Module Ports Configuration

4. Select All Module Ports Configuration. The All Ports Configuration dialog box opens (Figure 5-15).

Figure 5-15. All Ports Configuration Dialog Box



5. Select the check box next to the field you want to configure.
6. Select an option for the specific field from that fields pull-down menu.
7. Select Restore to keep the previous settings or Apply to accept the new settings.

6 Managing the Address Forwarding Table

Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- Configuring the Address Forwarding Table (AFT)
- Searching the Switch AFT
- Adding Entries to the AFT Manually

Configuring the Address Forwarding Table (AFT)

You can configure the following AFT parameters:

- **Address Age Time -** defines the length of time addresses remain active in the address forwarding table.
- **Super Age Time** - defines how long inactive addresses are stored in the address forwarding table before being deleted.
- **Address Table Sizing Parameters** - allow you to adjust what the switch does when address table use becomes inefficient.

Also provided is information that is useful when working with Avaya support personnel.

Configuring the Age Timer and Super Age Timer

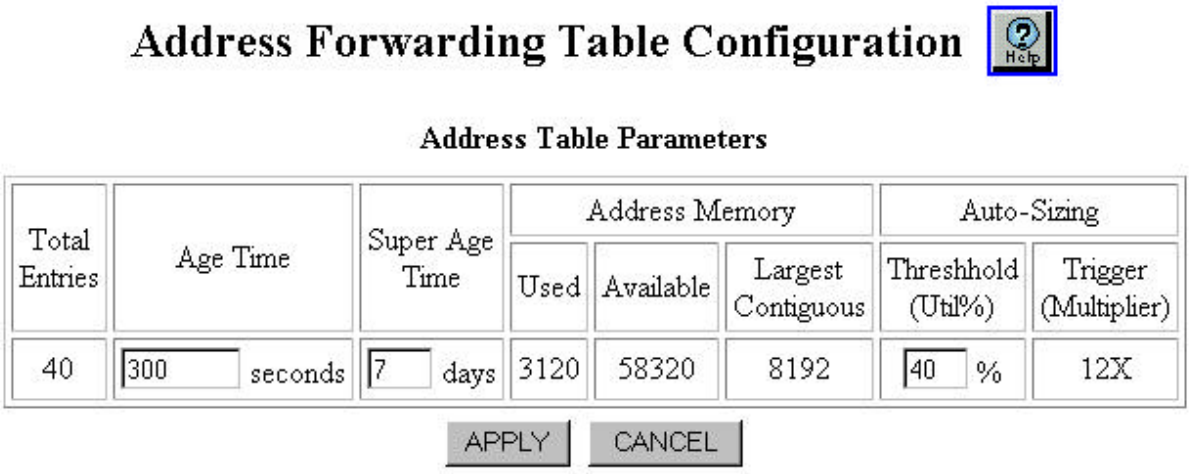
You can configure the Age Timer and Super Age Timer using either the web agent or the CLI.

Configuring the Age Timer and Super Age Timer Using the Web Agent

To change the aging values for all instances of the address table using the web agent:

1. Select Table Configuration from the Address Forwarding Table group in the Web Agent window. The Address Forwarding Table Configuration dialog box opens (Figure 6-1).

Figure 6-1. Address Forwarding Table Configuration Dialog Box



2. Enter a value in the Age Time field. Aged out addresses become invalid until the switch sees another packet with the aged out entry's source address.The standards-recommended default is 300 seconds.

3. Enter a new value in the Super Age Time field. The Super Age Timer marks all invalid table entries, then checks to see if they remain invalid for the specified super age interval. This clears the table of entries that are no longer used. The default value is 7 days.

4. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring the Age Timer and Super Age Timer Using the CLI

To change the aging values for all instances of the address table using the CLI, enter one of the following commands from **Configure** mode:

```
> set aft agetime <age-time-value>
> set aft super-agetime <age-time-value>
```

Refer to the *Avaya™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Controlling Reconfiguration of AFT Sizes

Each VLAN you define creates a separate version of the switch AFT. When these address tables become large, they may begin to use address space inefficiently.

By default, the hash table (AFT Instance) has auto-increment (hash table size) on. This means that when a hash table either can't add a new entry or the utilization of the space in the hash table was poor, that the hash table would automatically increment its size (thereby deleting all learned entries). This new size is kept in NVRAM so that when the box reboots, it doesn't have to go through the resizing process again, instead the new size is used.

You may specify that auto-increment be disabled on a per-AFT Instance basis if they wish for the hash table to remain a constant size. The problem is how to determine that you have "poor" utilization. Bucket Utilization is the number of AFT entries divided by the total AFT bucket space (times 100 for a percentage). Buckets only come in sizes that are multiples of 2 from 1 to 128. Therefore, if you have 5 entries to put in a bucket, the best you can do is put it in a bucket of size 8 with 62.5% utilization for that bucket. It may be the case, however, that you can only fit those 5 entries in a bucket of size 16 (because of hashing difficulties), yielding 31.25% utilization for that bucket. If you have low total utilization, you can almost always get better utilization by increasing the size of the hash table (simply because there will be less hash collisions to resolve in buckets).

In the normal case, a hash table's utilization starts very high, and then begins to decrease as more entries are added. The Utilization Threshold is the point at which, if Hash Table Auto-Incrementing is enabled, the hash table will increment its size automatically. Therefore if it is set to 40%, then say the utilization starts dropping down from 100%, when it reaches 40%, then it will auto-increment its size.

However, there is one more catch: the Trigger. The Trigger is a multiplier. Simply put, before the utilization is even looked at to determine if we should auto-increment the hash table size, there must be a minimum number of AFT entries in the hash table. That minimum number is the size of the hash table times the Trigger Multiplier. E.g. Since the Trigger Multiplier is 12, if the hash table size is 1k, then there must be at least 12k entries in the table before utilization will be looked at to determine whether we should auto-increment the size of the hash table. The Trigger Multiplier sets a lower bound so that we do not keep incrementing the hash table size because of a small number of entries that cannot be resolved into a small bucket.

You can control when a flood event occurs using either the web agent or the CLI.

Controlling Reconfiguration of AFT Sizes Using the Web Agent

To manually control reconfiguration of AFT sizes using the web agent:

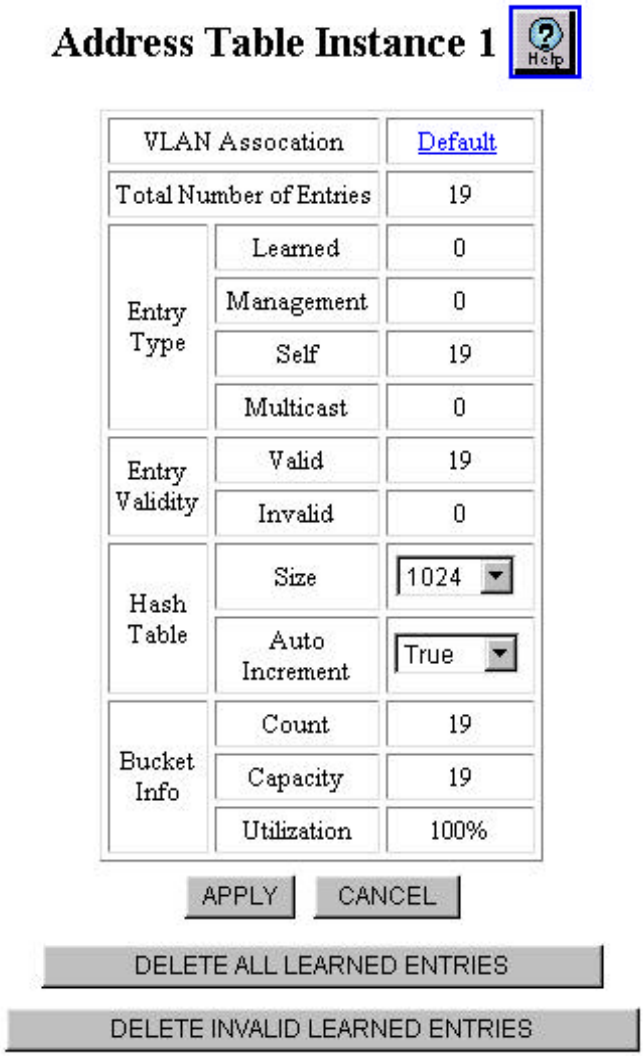
1. Select Table Configuration from the Address Forwarding Table group in the Web Agent window. The Address Forwarding Table Configuration dialog box opens (Figure 6-1).

2. Enter a new Auto-Sizing Utilization Threshold percentage in the Threshold (Util%) field, if you just want to cause the table reconfiguration to occur at a different level of usage efficiency. The default value of 40% is recommended for most applications.

   ***Note:** Raising the value in the Threshold (Util%) field might cause the table to be relearned more frequently, and makes address space usage more efficient.

3. Select the ID number to achieve finer control of particular tables in the Instance ID column. The Address Table Instance dialog box opens for the instance ID selected (Figure 6-2)

Figure 6-2. Address Table Instance Dialog Box



4. Refer to Table 6-1 for a definition of the Address Table Instance dialog box parameters.

Table 6-1. Address Table Instance Parameters

Parameter	Definition
VLAN Association	Displays the associated VLAN switch port and opens the VLAN Switch Port dialog box.
Total Number of Entries	Displays the total number of entries for this VLAN.
Entry Type	Displays the entry type for this VLAN. Options include: • **Learned** - Entry is dynamically learned. • **Management** - Entry is configured by the user statically. • **Self** - Entry is the switch's own address • **Multicast** - Entry is a multicast address.
Entry Validity	Displays the entry validity for this VLAN. Options include: • **Valid** - Entry exists. • **Invalid** - Entry has aged out but still exists even though the port binding is invalid.

Table 6-1. Address Table Instance Parameters continued

Parameter	Definition
Hash Table	Select one of the following hash table parameters: **Note:** **Size** - Select the size to alter the space available for this address table. The selection range is 16 addresses to 8192 addresses. The rule of thumb is: Tables with high Total Bucket Utilization (greater than 75%) can be made smaller. Tables with low Total Bucket Utilization (less than 40%) should be made larger. **Note:** The number of addresses for a given hash table is 4:1 (for example, if you have a hash table of 16 bytes, the VLAN can hold 64 addresses in it's table instance. It is recommended that the hash table size be 1/8th the size of the total number of addresses for the VLAN. • **Auto Increment** - Select an option to allow the Hash tables to grow dynamically larger if more addresses are discovered. The options are: **True** _ Enables auto-increment of the Hash tables. **False** - Disables auto-increment to prevent the Hash tables from growing dynamically at the risk of extra flooding.
Bucket Info	Displays parameters to monitor the efficiency of the hash table allocations. Options include: • **Count** - Indicates the hash table count. • **Capacity** - Indicates the hash table capacity. • **Utilization** - High utilization indicates that a larger hash table is needed.

5. Click:

- **APPLY** to save your changes
- **CANCEL** to restore previous settings
- **Delete All Learned Entries if** you want to relearn the entire table
- **Delete Invalid Learned Entries** if you want to delete all entries that are currently aged out.

*** Note:** If you change the Hash Table Size, the switch relearns all addresses in that table, causing the switch to flood packets for a few seconds.

Controlling Reconfiguration of AFT Sizes Using the CLI

To manually control reconfiguration of AFT sizes using the CLI, enter the following command in **Priv** mode:

```
> set aft auto-sizing-threshold
```

Refer to the *Avaya™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Searching the Switch AFT

The AFT can hold more than 24,000 entries on each switch. The switch Web Agent provides a utility that allows you to filter which addresses it displays, making the list more manageable. Multiple criteria can be selected to produce a sophisticated filter. The parameters are treated as "ands," meaning that displayed addresses must meet all selected criteria.

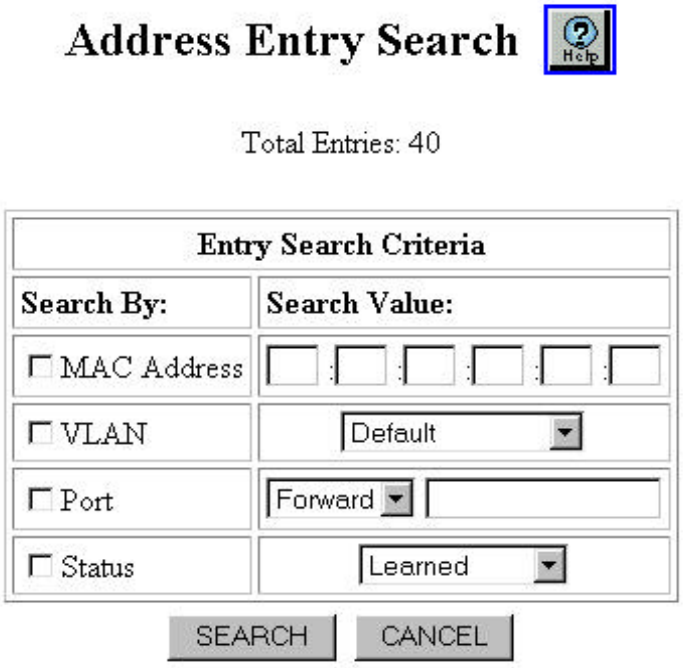
You can search the AFT using the web agent or the CLI.

Searching the Switch AFT Using the Web Agent

To filter the AFT using the web agent:

1. Select Entry Search from the Address Forwarding Table group on the web agent window. The Address Entry Search dialog box opens (Figure 6-3)

Figure 6-3. Address Entry Search Dialog Box.



***Note:** A search ignores any parameter not checked in the left column. To view all addresses in the table, select Search without selecting any filters.

2. To search using a MAC Address:

— Select the MAC Address checkbox in the Search By: column

— Enter a MAC address in the Search Value column.

***Note:** You only have to enter a portion of the MAC address.

3. To search using a VLAN:

— Select the VLAN checkbox in the Each By: column

— Select a VLAN name from the VLAN field pull-down menu in the Search Value column.

4. To search using a Port:

— Select the Port checkbox in the Search By: column

— Select a search variable from the Port field pull-down menu. The options are: Forward, Filter, and CPU

— Enter a port number to display only the entries associated with that switch port.

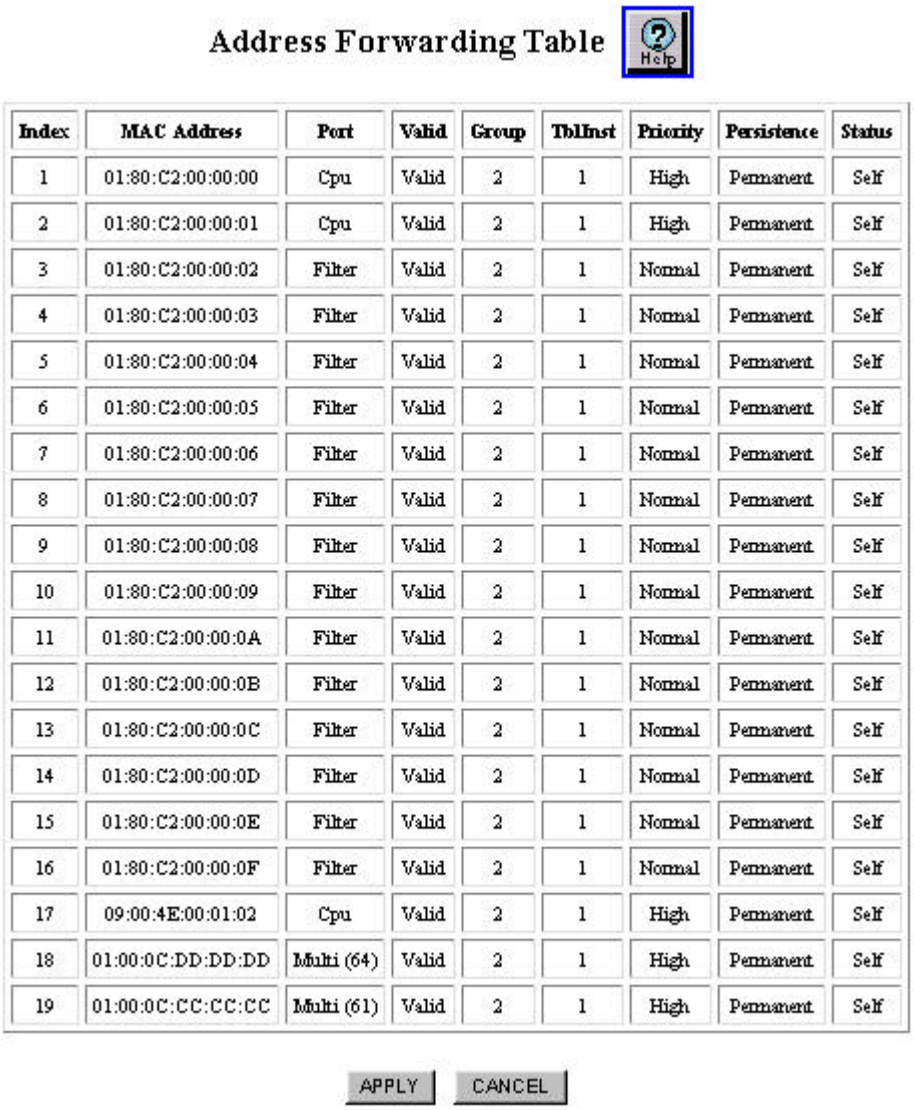
5. To search using a bridging status:

— Select the Status checkbox in the Search By: column

— Select a status from the pull-down menu to show only ports of a specific bridging status. The options are Learned, Management, Self, and Multicast.

6. Select SEARCH to open the Address Forwarding Table dialog box (Figure 6-4).

Figure 6-4. Address Forwarding Table Dialog Box



Index	MAC Address	Port	Valid	Group	TblInst	Priority	Persistence	Status
1	01:80:C2:00:00:00	Cpu	Valid	2	1	High	Permanent	Self
2	01:80:C2:00:00:01	Cpu	Valid	2	1	High	Permanent	Self
3	01:80:C2:00:00:02	Filter	Valid	2	1	Normal	Permanent	Self
4	01:80:C2:00:00:03	Filter	Valid	2	1	Normal	Permanent	Self
5	01:80:C2:00:00:04	Filter	Valid	2	1	Normal	Permanent	Self
6	01:80:C2:00:00:05	Filter	Valid	2	1	Normal	Permanent	Self
7	01:80:C2:00:00:06	Filter	Valid	2	1	Normal	Permanent	Self
8	01:80:C2:00:00:07	Filter	Valid	2	1	Normal	Permanent	Self
9	01:80:C2:00:00:08	Filter	Valid	2	1	Normal	Permanent	Self
10	01:80:C2:00:00:09	Filter	Valid	2	1	Normal	Permanent	Self
11	01:80:C2:00:00:0A	Filter	Valid	2	1	Normal	Permanent	Self
12	01:80:C2:00:00:0B	Filter	Valid	2	1	Normal	Permanent	Self
13	01:80:C2:00:00:0C	Filter	Valid	2	1	Normal	Permanent	Self
14	01:80:C2:00:00:0D	Filter	Valid	2	1	Normal	Permanent	Self
15	01:80:C2:00:00:0E	Filter	Valid	2	1	Normal	Permanent	Self
16	01:80:C2:00:00:0F	Filter	Valid	2	1	Normal	Permanent	Self
17	09:00:4E:00:01:02	Cpu	Valid	2	1	High	Permanent	Self
18	01:00:0C:DD:DD:DD	Multi (64)	Valid	2	1	High	Permanent	Self
19	01:00:0C:CC:CC:CC	Multi (61)	Valid	2	1	High	Permanent	Self

7. Click APPLY to save the current settings, CANCEL to restore previous settings. or MORE to view more statistics.

8. Refer to Table 6-2 to review your search criteria options:

Table 6-2. Address Forwarding Table Parameters

Parameter	Defines the...
Index	Index number of this address entry in the switch address forwarding table.
MAC Address	MAC address associated with this entry. This address is learned by the switch as an address to forward to the associated port.
Port	Port associated with this MAC address table entry. Use this setting to display the entries associated with that port. Options include: • **Forward** - Forwards the entry. • **Filter** - Filters the entry. • **Cpu** - Stores the entry.
Valid	Whether the port binding is valid. This helps the re-learn performance.
Group	Group number associated with this MAC address.
TblInst	Address table instance number associated with this MAC address.
Priority	Priority level associated with traffic forwarded to this MAC address. The options are: • **Normal** • **High** You can set this parameter on all learned entries.

***Table 6-2. Address Forwarding Table Parameters** continued*

Parameter	Defines the...
Persistence	The persistence of the entry in the table can be set on all learned entries: • **Permanent -** The address is not aged out of the table. • **Invalid -** This entry is cleared from the table each time the switch resets. • **Ageout -** Address is cleared from the address forwarding table when the timeout interval expires. This is the state of all entries dynamically learned by the switch. It ensures that MAC addresses that are not active on the network do not remain in the switch address forwarding table indefinitely.
Status	The status of the address entry. Options include: • Learned • Management • Self • Multicast

Searching the Switch AFT Using the CLI

To search the switch AFT using the CLI, enter the following command in Priv mode:

```
Cajun# show aft entry (CR, mac, port-binding,
status, vlan)
```

Refer to the *Avaya™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Adding Entries to the AFT Manually

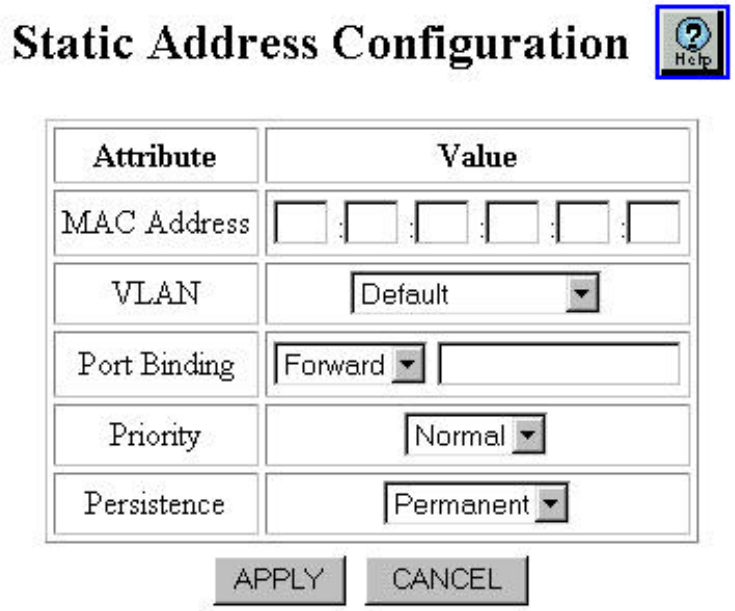
You can add entries to the AFT manually using the web agent or the CLI to ensure they remain permanent.

Adding Entries to the AFT Manually Using the Web Agent

To add an AFT address manually using the web agent:

1. Select Entry Configuration from the Address Forwarding Table group in the Web Agent window. The Static Address Configuration dialog box opens (Figure 6-5).

Figure 6-5. Static Address Configuration Dialog Box.



2. Enter the MAC address that you want to add to the table in the MAC Address Value field.
3. Select a VLAN for this entry from the VLAN field pull-down menu.
4. Select Forward or Filter from the Port Binding field pull-down menu.
5. Enter the port that you want associated with this entry in the Port Binding field.

6. Select a priority level from the Priority field pull-down menu for packets that you want forwarded to this MAC address. High priority addresses move to the front of the switch packet buffers automatically.

7. Select Persistence or Ageout from the Persistence field pull-down menu.

8. Refer to Table 6-3 for an explanation of the Aging and Persistence field parameters:

Table 6-3. Entry Persistence

Parameter	Definition
Permanent	The address is saved in nonvolatile memory and is not aged out of the table.
Ageout	Address is cleared from the address forwarding table when the timeout interval expires. This is the state of all entries dynamically learned by the switch. It ensures that MAC addresses that are not active on the network do not remain in the switch address forwarding table indefinitely.

9. Click APPLY to save your changes, or CANCEL to clear the dialog box fields.

Adding Entries to the AFT Manually Using the CLI

To add entries to the AFT manually using the CLI, enter the following command in Configure mode:

```
cajun(configure)# set aft entry (mac address)
```

Refer to the *Avaya™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

7 Configuring Redundancy Options

Overview

The following information and procedures are provided in this chapter and are common to both layer 2 and layer 3 module configuration:

- Configuring Redundant Hardware
- Installing Redundant Hardware
- Enabling Redundant Hardware
- Configuring a Redundant CPU

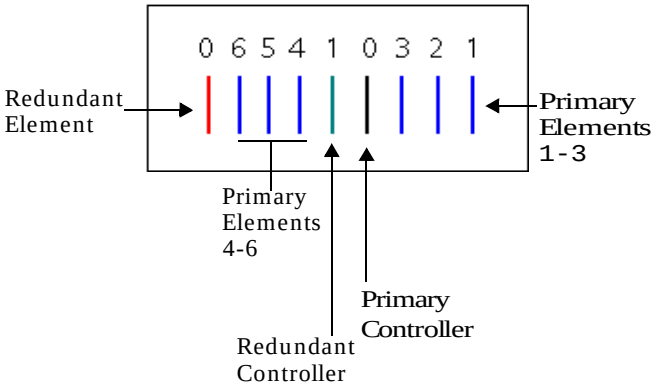
Configuring Redundant Hardware

All three switches (layer 2 and layer 3 models) provide a redundant backplane to ensure that should a supervisor module or a fabric element fail, it will continue to route data properly. The redundant components are available as separate options.

When the redundant controller and element are installed, the backplane consists of the following parts (Figure 7-1):

- One Primary Controller
- One Redundant Controller
- Six Primary elements
- One Redundant element

Figure 7-1. Layout of the Redundant Backplane



All three switches are equipped with diagnostics to monitor the status of the primary, redundant, and switch controllers, and the primary elements. If the primary supervisor fails, the redundant supervisor takes over switch operation until you replace the primary supervisor. If the primary controller fails, the redundant controller takes over switch operation until you replace the primary controller. Information about a failed supervisor (CPU) displays in the Redundancy window.

When an element fails, diagnostics run automatically and test the hardware. Information about a failed controller or element displays in the Switch Fabric Status window in the Web Agent. The redundant element takes over the function of the failed element until you replace the element.

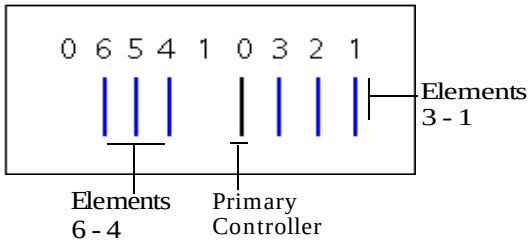
The following sections provide the following information:

- Installing Redundant Hardware
- Replacing the Primary Controller
- Replacing an Element
- Configuring a Redundant CPU

Installing Redundant Hardware

The standard switch configuration does not include is a redundant controller or element (Figure 7-2).

Figure 7-2. Default Hardware Configuration



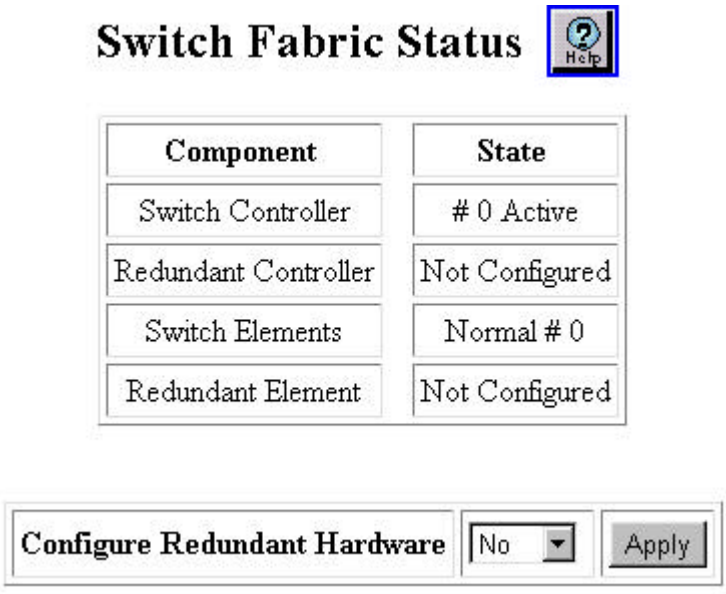
To install the redundant modules:

1. Power off all of the switch power supplies.
2. Install the redundant controller into the slot to the left of the primary controller. (Slot 1 in Figure 7-2).

   *** Note:** Controllers and elements are keyed to ensure that a controller is not inserted into an element slot and vice-versa.

3. Install the redundant element in the slot to the left of the sixth element. (Slot 0 in Figure 7-2).
4. Power on the switch power supplies and login.
5. Select **Switch Fabric** from the **System > Configuration** group on the web agent window. The **Switch Fabric Status** dialog box opens showing that both the redundant controller and redundant Element are now available (Figure 7-3).

Figure 7-3. Switch Fabric Status Dialog Box



Enabling Redundant Hardware

6. You can enable the redundant hardware from either the Web Agent or the CLI. After you enable redundant hardware, the applicable redundant component takes over if either the primary controller or element fails.

Enabling Redundant Hardware Using the Web Agent

To enable the redundant hardware using the web agent:

1. Select **Yes** from the **Configure redundant Hardware field** pull-down menu on the Switch Fabric Status dialog box (Figure 7-3).
2. Click **APPLY**. The redundant hardware is enabled. Enabling Redundant Hardware Using the CLI

To enable the redundant hardware using the CLI, enter the following command from Priv Configure mode:

```
> set fabric configure-redundant-hardware enable
```

Refer to the *Avaya™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Replacing the Primary Controller

If a primary controller fails, you are notified by:

- A console message
- An event log message
- The following error message that displays in the **Switch controller** field on the **Switch Status** dialog box:

  `> # 0 Failed`

If the switch is installed with a redundant controller that has been enabled, the redundant controller automatically takes over the operation of the failed primary controller.

To replace the primary controller:

1. Select **Switch Fabric** from the **System > Configuration** group on the web agent window. The **Switch Fabric Status** dialog box opens (Figure 7-3).
2. Select No from the **Configure Redundant Hardware** field pull-down menu.
3. Click **APPLY** to disable the primary controller.
4. Power off the switch power supplies.

WARNING

To avoid bodily harm and equipment damage, you must power off the switch before you remove switch controllers or elements.

5. Remove the failed primary controller from the switch.
6. Replace with a good primary controller.
7. Power on the switch power supplies and login.
8. Refer to the "Enabling Redundant Hardware" section and complete the procedure.
9. Re-select **Switch Fabric** from the **System > Configuration** group on the web agent window. The **Switch Fabric Status** dialog box re-displays with the Switch Controller field displaying:

   `# 1 Active`

Replacing an Element

If an element fails, you are notified by:

- A console message
- An event log message
- An error message that displays in the **Switch Elements** field on the Web Agent **Switch Status** window:

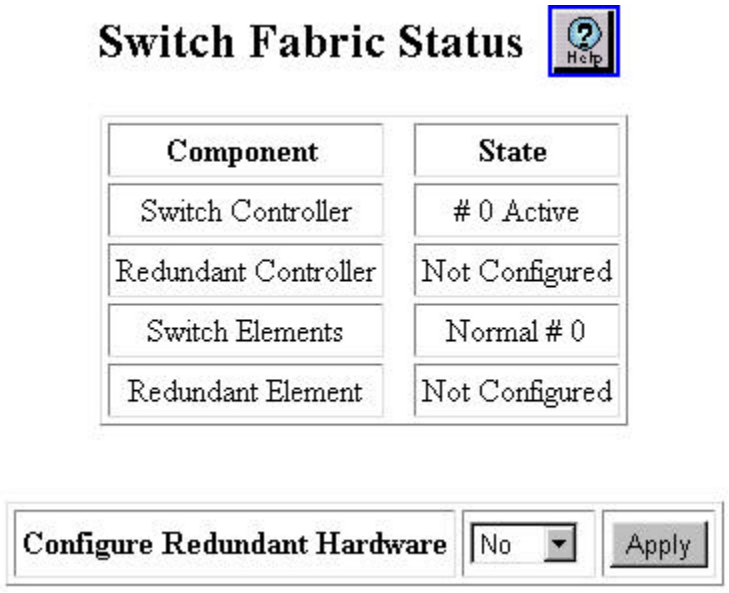
  `# Failed <number>`

where `<number>` is the number that indicates the failed element.

To replace an element:

1. Select Switch Fabric from the System> Configuration group on the web agent window. The Switch Fabric Status dialog box opens (Figure 7-4).

Figure 7-4. Switch Fabric Status Dialog Box



2. **Select No from the Configure Redundant Hardware field pull-down menu.**
3. **Select APPLY to disable the failed element.**

4. Power off the switch.

WARNING

To avoid bodily harm and equipment damage, you must power off the switch before you remove switch controllers or elements.

5. Remove the failed element from the switch.
6. Replace a good element into the switch.
7. Power on the switch's power supplies and login.

Enabling a Replaced Element Using the Web Agent

To enable a replaced element using the web agent:

1. Select Switch Fabric from the System> Configuration group on the web agent window. The Switch Fabric Status dialog box opens (Figure 7-4).
2. Select Yes from the Configure Redundant Hardware field pull-down menu.
3. Click APPLY to enable the redundant element.

   The Switch Elements field displays:

   ```
   Normal # 0
   ```

   This indicates that the redundant element is now enabled.
4. Select Normal from the Enable redundant Element field pull-down menu.
5. Click **APPLY**.

Enabling a Replaced Element Using the CLI

To enable a replaced element using the CLI, enter the following command from Configure mode:

```
> set fabric configure-redundant-hardware
{enable|disable}
```

Refer to the *Avaya P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Configuring a Redundant CPU

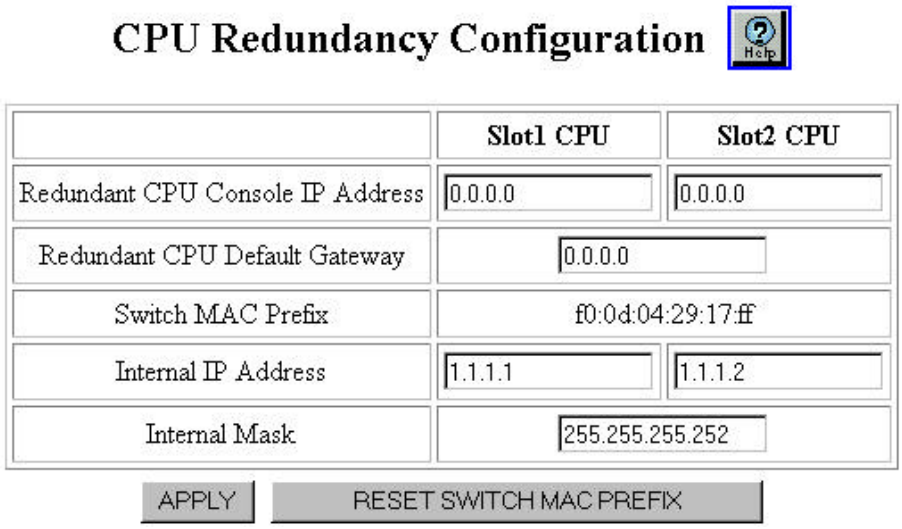
If your Primary CPU fails, the redundant CPU takes control of network operation immediately. You are notified of this change by a console message and an event log message. You can configure the redundant CPU using the web agent or the CLI.

Configuring a Redundant CPU Using the Web Agent

To configure a redundant CPU using the web agent:

1. Select Configuration from the System> Configuration > CPU Redundancy group on the web agent window. The CPU Redundancy Configuration dialog box opens (Figure 7-5)

Figure 7-5. CPU Redundancy Configuration Window



2. Enter the Internal IP address for the redundant CPU in the Internal IP Address field under Slot2 CPU.
3. Enter the subnet mask in the Internal Mask field. The default value is 255.255.255.0.
4. Click APPLY to save your changes.

Configuring a Redundant CPU Using the CLI

To configure a redundant CPU using the CLI by entering the following command from Configure mode:

```
> cpu_redundancy console slot2 <ip address>
```

Refer to the *Avaya P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Synchronizing the Primary and Redundant CPUs

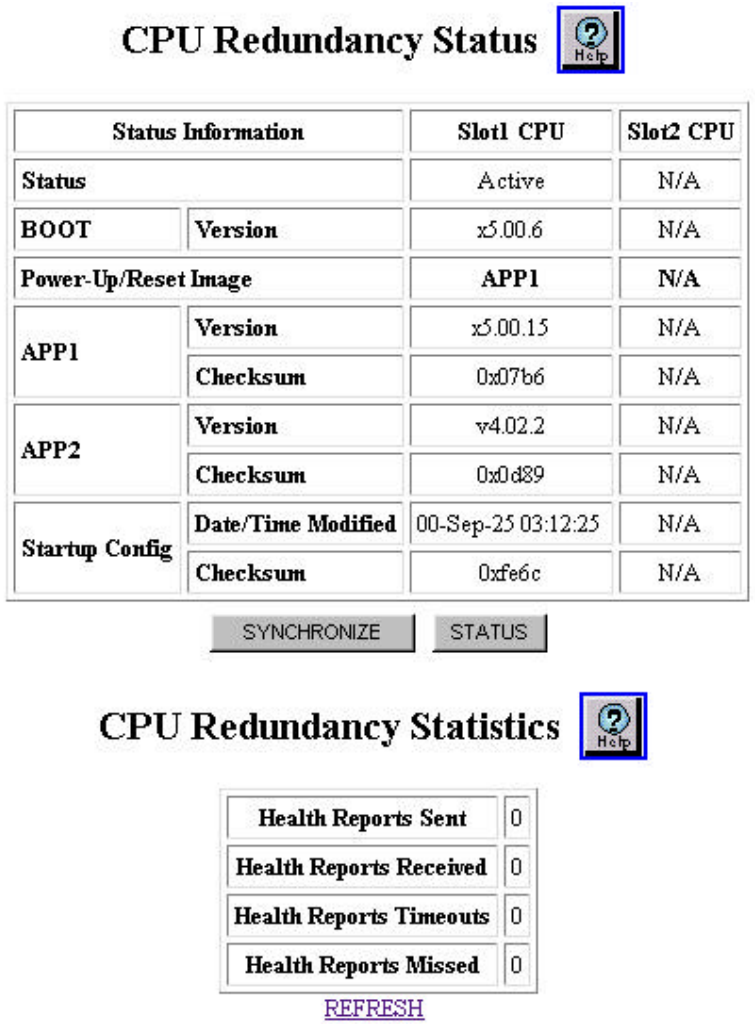
You must synchronize the Primary and redundant CPUs after you configure both. You can synchronize both CPUs using the web agent or the CLI.

Synchronizing the Primary and Redundant CPUs Using the Web Agent

To synchronize the Primary and redundant CPU's using the web agent:

1. Select Status/Statistics from the System> Configuration> CPU Redundancy group on the web agent window. The CPU Redundancy Configuration dialog box opens (Figure 7-6).

Figure 7-6. CPU Redundancy Status



2. Sychronize the Primary and redundant CPUs. Refer to Table 7-1 for more information on the CPU configuration dialog box parameters).

Table 7-1. CPU Redundancy Configuration Information

Parameter	Definition
Status	Displays the functional status of the CPU modules.
Power-Up/ Reset Image	Displays the running configuration image for each CPU module.
APP1	• **Version** - Displays the current running version of application 1 (APP1) for each CPU module. You must use version 5.0 or greater in order to make use of the router redundancy protocol. • **Checksum** - Displays the TBD
APP2	• **Version** - Displays the current running version of application 2 (APP2) for each CPU module. You must use version 5.0 or greater in order to make use of the router redundancy protocol. • **Checksum** - Displays the TBD
Startup Config	• **Date/Time Modified** - Displays the date and time that the configuration (startup.txt) was modified. • **Checksum** - Displays the TBD.

3. Click SYNCHRONIZE to save the synchronization images and configurations, or STATUS to refresh the status information for both the Primary and redundant CPUs.

Synchronizing the Primary and Redundant CPUs Using the CLI

To synchronize the Primary and redundant CPU's using the CLI. enter the following command in Priv mode:

```
> # cpu_redundancy sychronize
```

Refer to the *Avaya P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

8 Configuring DNS and RADIUS Clients

Overview

The following information and procedures are provided in this chapter and are common to both layer 2 and layer 3 module configuration:

- Configuring a Domain Name System (DNS) Client
- Configuring a Remote Authentication Dial-In User Service (RADIUS) Client

Configuring a Domain Name System (DNS) Client

The Domain Name System (DNS) is a distributed database of name servers which supply name-to-address translations. The root name servers at the top of the DNS database tree contain pointers to the master name servers for each of the top-level domains. The master name servers contain pointers to the individual name servers for each of the subdomains within its top-level domain. The individual name servers contain detailed address information for the local hosts in the subdomain.

For minimum operation of DNS, you must enable DNS and specify at least one name server IP address. You may specify a default domain name suffix, but it is not required. If you do not specify a domain name, you must enter a fully qualified host name, for example: *jerry.avaya.com*. If the default domain name suffix was already specified (for example: *Avaya.com*), you only have to enter a simple host name (for example: *jerry*).

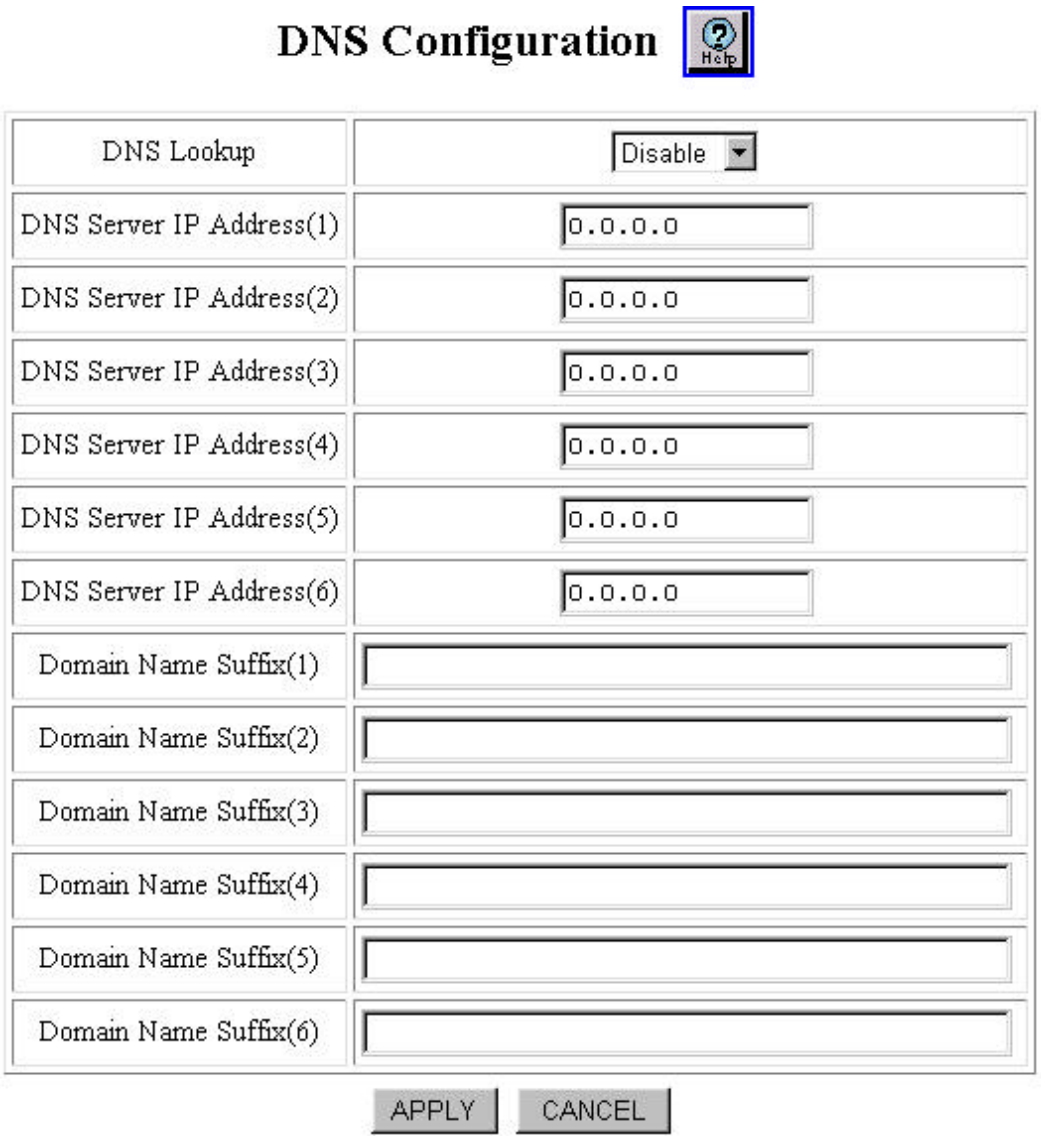
You can configure DNS using either the web agent or the CLI.

Configuring a DNS Client Using the Web Agent

To configure a DNS client using the web agent:

1. Select DNS from System> Administration group on the web agent window. The DNS Configuration dialog box opens (Figure 8-1).

Figure 8-1. DNS Configuration Dialog Box



2. Select Enable from the DNS Lookup field pull-down menu to enable DNS on the switch.

3. Enter the DNS server IP address for each DNS server in the DNS Server IP Address fields (fields 1-6).
4. Enter the domain name suffix for each DNS server in the Domain Name Suffix fields (fields 1-6).
5. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring a DNS Client Using the CLI

To configure a DNS client using the CLI, enter the following command from Configure mode:

```
> ip domain-name <dns name>
```

Refer to the *Avaya P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

Configuring a Remote Authentication Dial-In User Service (RADIUS) Client

A RADIUS client provides a mechanism for consolidating user login information. RADIUS is a mechanism used for authenticating remote users who log into a switch. You can log into the switch in order to view or manage the switch through the embedded web agent or the CLI.

When a user attempts to log into the switch, if there is no local user account for the entered user name and password, the switch sends an Authentication Request to the RADIUS server in an attempt to authenticate the user remotely. If the user name and password are authenticated, then the RADIUS server responds with an Authentication Acknowledgement that includes information on the user's privileges and the user is allowed access to the switch. If the user is not authenticated, then a Authentication Reject is sent to the switch and the user is denied access to the switch's embedded management.

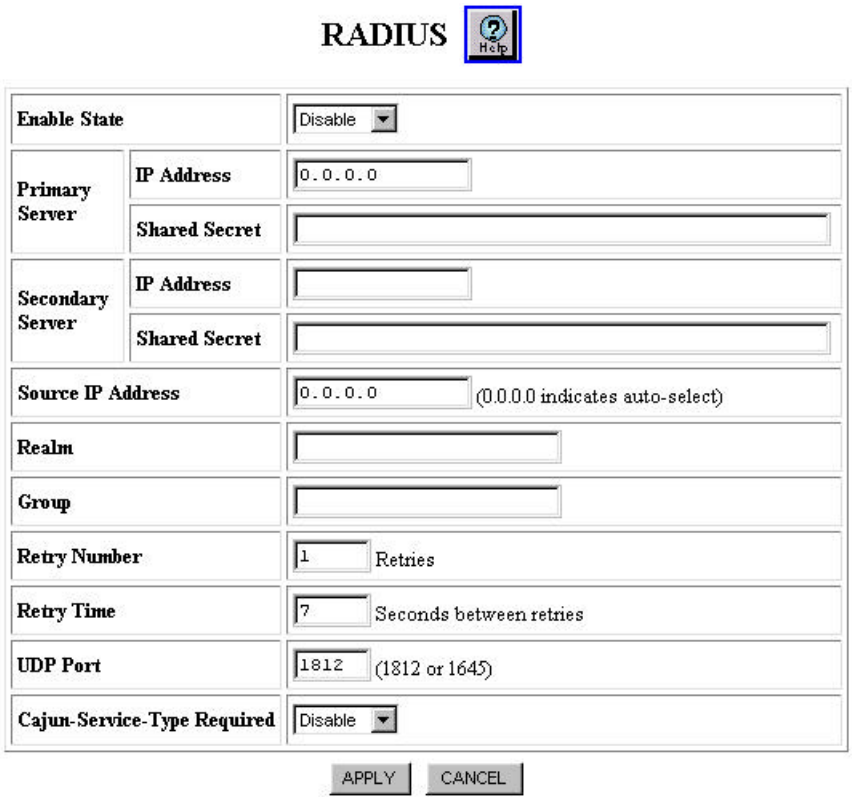
You can configure a RADIUS client using either the web agent or the CLI.

Configuring a RADIUS Client Using the Web Agent

To configure a RADIUS client using the web agent:

1. Select RADIUS from the System > Administration group on the Web Agent window,. The RADIUS dialog box opens (Figure 8-2).

Figure 8-2. RADIUS Dialog Box.



2. Select Enable from the Enable State field pull-down menu.

3. Refer to Table 8-1 to configure the RADIUS dialog box configuration parameters;

Table 8-1. RADIUS Dialog Box Configuration Parameters

Parameter	Definition
Enable State	Enable or disable RADIUS on the switch.
Primary Server	• **IP Address** - Enter the primary server IP address for RADIUS. • **Shared Secret** - Enter the primary server shared RADIUS secret. This value is encrypted.
Secondary Server	• **IP Address** - Enter the secondary server IP address for RADIUS. • **Shared Secret** - Enter the secondary server shared RADIUS secret. This value is encrypted.
Source IP Address	Enter the network access server IP address.
Realm	Enter an ASCII name that will differentiate users. This name will be appended to the user name.
Group	Enter an ASCII name that will differentiate group users.
Retry Number	Enter the number of times to re-send the Authentication Request if there is no response.
Retry Time	Enter the time (in seconds) to wait before re-sending an Authentication Request.
UDP Port	Enter the UDP port number. The default value is **1812**.
Avaya-Service-Type Required	Enable or disable whether the service type to be granted to a user is sent in an Access-Accept packet. This setting ensures that the switch will not incorrectly allow access to users that may already be set-up on the RADIUS server.

Configuring a RADIUS Client Using the CLI

To configure a RADIUS client using the CLI, enter the following command from Configure mode:

```
> set radius authentication <parameters>
```

Refer to the *Avaya P500/P880/P882 Switch Command Line Interface Reference Guide* for more details about this command.

9 Configuring IP Routing

Overview

The following information and procedures provided in this chapter pertain to layer 3 module configuration only:

- Configuring Internet Protocol (IP) Global Routing
- IP Multicast
- Monitoring Switch Performance Using IP Statistics
- Configuring Virtual Redundant Router Protocol (VRRP)
- Configuring ICMP Router Discovery Protocol (IRDP)
- Configuring Lightweight Directory Access Protocol (LDAP)

Configuring Internet Protocol (IP) Global Routing

You can emulate bridging capabilities inside the P550 /P880/P882 Switch chassis through Virtual Local Area Networks (VLANs). Capabilities that once were provided by additional hardware, such as bridges, switches, and hubs, are now provided as virtual configurations inside the router. The ability to emulate bridging hardware through a virtual means is referred to as IP Routing. High-level tasks involved in creating and setting up IP Routing include:

- IP Multicast
- Monitoring Switch Performance Using IP Statistics
- Configuring Virtual Redundant Router Protocol (VRRP)
- Configuring ICMP Router Discovery Protocol (IRDP)
- Configuring Lightweight Directory Access Protocol (LDAP)

For information about creating and assigning physical ports to a VLAN, refer to Creating and Implementing VLANs, in Chapter 4.

The following sections explain how to enable IP routing and assign subnets.

Creating an IP Interface

When you create an IP interface, you activate a location in the switch that communicates between IP and the embedded software of the switch.

You can create an I{P interface using either the web agent or the CLI.

Creating an IP Interface Using the Web Agent

To create an IP interface using the web agent:

1. Select Interfaces from the Routing > IP > Configuration group on the web agent window. The IP Interfaces dialog box opens (Figure 9-2).

*** Note:** Due to the length of the IP Interfaces dialog box, it is shown as two figures in Figure 9-1.

Figure 9-1. IP Interfaces Dialog Box

IP Interfaces Help

Select	State	Interface	Admin. State	VLAN	Network Address	Mask	MAC Format	ARP Timeout
☐	UP	hforew	UP	Default	2.3.4.5	255.255.255.0	Ethernet V2	360
☐	UP	jerry	UP	Default	198.162.99.60	255.255.255.0	Ethernet V2	360
☐	UP	Internal-Network	UP	Internal-Network	10.2.2.1	255.255.255.240	Ethernet V2	360
☐	UP	192.168.99.60	UP	Ethernet-Console	192.168.99.60	255.255.255.0	Ethernet V2	360

APPLY CREATE DELETE CANCEL

IP Routing	RIP	OSPF	Multicast Protocol	Proxy ARP	ICMP Redirect	NetBIOS UDP Rebroadcast	VRRP	BOOTP/DHCP Relay Gateway
Routing/Mgmt	Disable	Enable	DVMRP	Disable	Enable	Disable	Disable	Disable
Routing/Mgmt	Disable	Disable	DVMRP	Disable	Enable	Disable	Disable	Disable
Mgmt Only	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable
Mgmt Only	Disable	Disable	N/A	Disable	Disable	Disable	Disable	Disable

2. Refer to Table 9-1 for an explanation of the IP Interfaces dialog box parameters.

Table 9-1. IP Interfaces Dialog Box Parameters

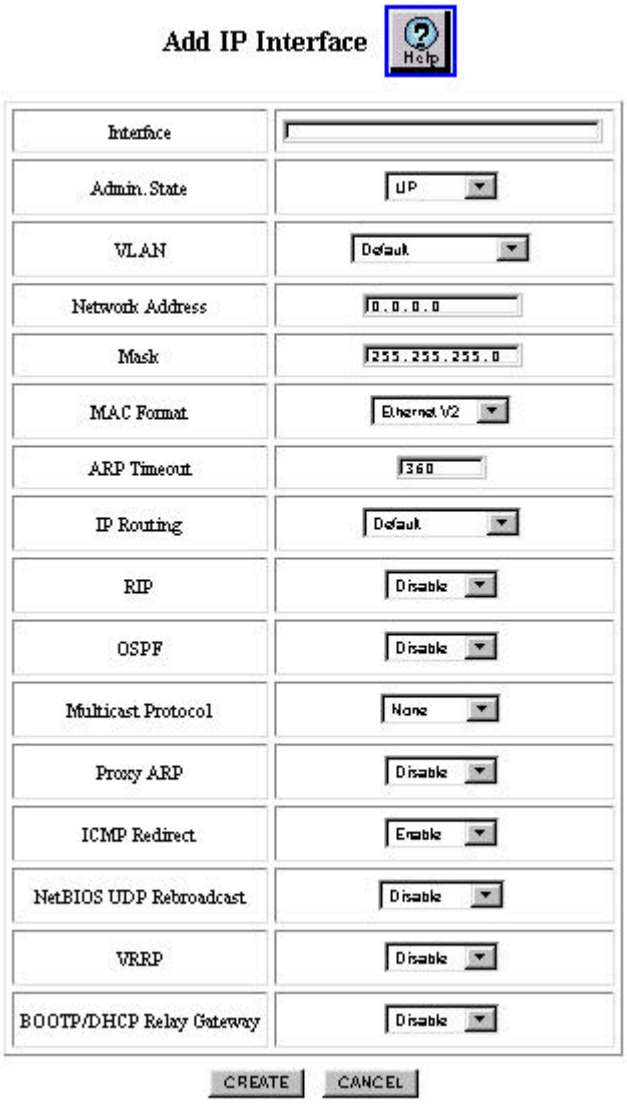
Parameter	Allows you to...
Select	Select the interface to configure.
State	Show the current running condition of the switch. Options include: • **UP** - The interface is active. • **DOWN** - The interface is inactive.
Interface	Enter an interface name from the interfaces you have previously configured.
Admin State	Shows the administration state of the interface. The default setting is UP. Options include: • **UP** - Indicates an active state. • **DOWN** - Indicates an inactive state.
VLAN	Select a VLAN associated with the selected interface from the VLANs you have previously configured.
Network Address	Assign an IP address to the VLAN you previously selected.
Mask	Assign a subnet mask for the interface.
MAC Format	Specify the MAC format (Ethernet V2 or SNAP).
IP Routing	Enable or disable IP Routing on the interface. When set to Routing/Mgmt, you can both manage the switch (from the CLI or Web Agent), and configure IP Routing for the switch. When set to Mgmt Only, you can manage the switch, however, IP routing is disabled. **Note:** When the interface has a VLAN identified as Serial-Console, the only valid IP routing option is Mgmt Only.
RIP	Enable or disable RIP for a given interface.
OSPF	Enable or disable OSPF for a given interface.
Multicast Protocol	Select a multicast protocol to associate with your interface. Selections include: DVMRP, IGMP, and None. IGMP is enabled automatically when DVMRP is selected.
Proxy ARP	Enable or disable Proxy ARP on a given interface.
ICMP Redirect	Enable or disable Internet Control Message Protocol (ICMP) Redirect on a given interface.

***Table 9-1. IP Interfaces Dialog Box Parameters** continued*

Parameter	Allows you to...
NetBIOS UDP Rebroadcast	Configure your switch for InterVLAN forwarding of NetBIOS broadcasts. NetBIOS parameters include: • **Inbound** - Allow the receipt of NetBIOS requests. • **Outbound** - Allow the transmission of NetBIOS broadcasts. • **Both** - Allow the interface to both receive NetBIOS requests and send NetBIOS broadcasts. • **Disable** - Disallow both the receipt of NetBIOS requests and the transmission of NetBIOS broadcasts.
VRRP	Enable or disable VRRP on a given interface. The default value is Disable.
BOOTP/DHCP Relay Gateway	Enable or disable the BOOTP/DHCP Relay Agent. The default value is Disable.

3. Select CREATE from the bottom of the IP Interfaces dialog box. The Add IP Interface dialog box opens (Figure 9-2).

Figure 9-2. Add IP Interface Dialog Box.



4. Refer to Table 9-2 to configure the Add IP Interface dialog box parameters.

Table 9-2. Add IP Interface Dialog Box Parameters

Parameter	Allows you to...
Interface	Enter a unique, alphanumeric name for the interface.
Admin. State	Specify the administrative state of the interface. Options include: • **UP** - The interface is active. • **DOWN** - The interface is inactive.
VLAN	Specify the type of VLAN. Options include: • **Default** - Selects the default VLAN. • **Discard** - Selects the VLAN to be discarded. • **Ethernet-Console** - Selects the Ethernet Console port as the VLAN. • **Serial Console** - Selects the Serial Console port as the VLAN. **Note:** The way that you configure a VLAN to a port determines the IP Routing option that you select for the interface. Use the following options to configure the appropriate interface: • If you select to create an IP interface for an Ethernet-Console VLAN, select **Mgmt Only** from the IP Routing pull-down menu. • If you select to create an IP interface for a serial-console VLAN, select **Mgmt Only** from the IP Routing pull-down menu. • If you create an IP interface for an inbound VLAN, select **Routing Mgmt** from the IP Routing pull-down menu.
Network Address	Enter the network IP address for the selected interface.
Mask	Enter the subnet mask for the interface.
MAC Format	Select the MAC address format for the interface. Options include: • Ethernet V2 • Simple Network Access Protocol (SNAP)

Table 9-2. Add IP Interface Dialog Box Parameters continued

Parameter	Allows you to...
IP Routing	Select enable or disable IP routing on the interface. Options include: • **Routing/Mgmt** - Enables you to manage the switch, from the Command Line Interface (CLI) or the Web Agent, and configure IP routing for the switch. • **Mgmt Only** - Enables you to manage the switch, however, IP routing is disabled. • **Default** - Enables you to configure IP routing for the switch, however, you cannot manage the switch. **Note:** When you set up IP routing for an interface, the Default selection is automatically chosen. The IP interface is created with the default IP routing option on the VLAN associated with the interface.
RIP	Enable or disable RIP. The default value is Disable.
OSPF	Enable or disable OSPF. The default value is Disable.
Multicast Protocol	Specify the multicast protocol for the interface. Options include: • None • DVMRP • IGMP
Proxy ARP	Enable or disable Proxy ARP. The default value is Disable.
ICMP Redirect	Enable or disable ICMP Redirect (IDRP). The default value is Enable.
NetBIOS UDP Rebroadcast	Enable or disable NetBIOS UDP Rebroadcasts. The default value is Disable.
VRRP	Enable or disable Virtual Redundancy Router Protocol. The default value is Disable.
BOOTP/DHCP Relay Gateway	Enable or disable the BOOTP/DHCP Relay Agent. The default value is Disable.

5. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating an IP Interface Using the CLI

To create an IP interface using the CLI, enter the following command in Configure mode:

```
cajun(configure)# ip address <ip-address> <mask>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Enabling IP Routing

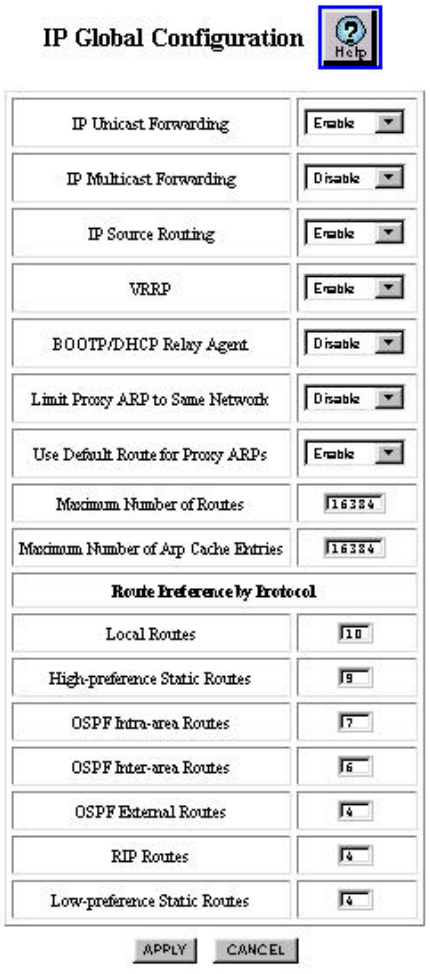
You can enable IP Routing using either the web agent or the CLI.

Enabling IP Routing Using the Web Agent

To enable IP routing using the web agent:

1. Select Global Configuration from the Routing > IP > Configuration group on the web agent window. The IP Global Configuration dialog box opens (Figure 9-3).

Figure 9-3. IP Global Configuration Dialog Box.



2. Refer to Table 9-3 to configure the IP Global Configuration dialog box.

Table 9-3. IP Global Configuration Parameters

Parameter	Allows you to...
IP Unicast Forwarding	**Disable** IP Unicast. The default setting is **Enable**.
IP Multicast Forwarding	**Enable** IP multicast on a global basis. This affects all IP RIP interfaces set up to use multicast protocols. The default setting is **Disable**.
IP Source Routing	**Disable** IP source routing globally. The default setting is **Enable**.
VRRP	**Disable** VRRP globally. The default setting is **Enable**.
BOOTP/DHCP Relay Agent	**Disable** client requests for an IP address and forwards their requests to a server. This agent also relays responses from the server to the client. The default setting is **Enable**.
Limit Proxy ARP to Same Network	**Enable** Proxy ARP on the same network. When enabled, the router only responds to ARP requests when the source and target IP address are in the same IP network and different IP subnets. When disabled, the router only responds to ARP requests when the source and target IP address are in different networks. The default setting is **Disable**.
Use Default Route for Proxy ARPs	**Disable** the use of the default route on your Cajun switch as the route for Proxy ARPs. For example, if you have a default route configured to reach the 0.0.0.0 IP address, then any ARP request that does not match any of the other routes in your IP routing table will automatically go to this default route. The default setting is **Enable**.
Maximum Number of Routes	Enter the maximum number of routes that you want added to the routing table. The default number of routes is **16384**. **Note:** These routes refer only to IP Unicast entries.
Maximum Number of ARP Cache Entries	Enter the maximum number of ARP cache entries. ARP entries refers to the space available for the IP address table. When you increase the number of entries, it may cause the table to be relearned more frequently. Consequently, it will make address space usage more efficient. The default maximum number of entries is **16384**.
Route Preference by Protocol	This section describes the routing preferences set up according to the network administrator's preferences. These preferences are normally set up using the most to least trust. For example, local routes are normally considered to have *more trust* or a *higher preference*, while OSPF external routes are considered to have *less trust* or a *lower preference*. These preferences can be overridden, but careful consideration must be given when setting each.
Local Routes	Enter a preference value for local routes.

Table 9-3. IP Global Configuration Parameters continued

Parameter	Allows you to...
High-Preference Static Routes	Enter a preference value for high-level static routes.
OSPF Intra-area Routes	Enter an OSPF intra-area route. A lower number indicates a lower preference for the path.
OSPF Inter-area Routes	Enter the inter-area paths to destinations in other OSPF areas. These are discovered through the examination of received summary Link State Advertisements (LSA). Enter a number to specify your path cost. A lower number indicates a lower preference for the path.
OSPF External Routes	Enter the number of external paths to destinations external to the Autonomous System (AS). These are detected through the examination of received AS external LSAs. Enter a number to specify your path cost (preference). A lower number indicates a lower preference for the path.
RIP Routes	Enter the number of RIP routes to use the hop count as a metric. Hence, to specify a preference for a RIP route, you need to enter a lower number (path cost).
Low-Preference Static Routes	Enter a preference value for low-level static routes.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Creating an IP Interface Using the CLI

To create an IP interface using the CLI, enter the following command in configure mode:

```
cajun (configure)# ip address <ip-address> <mask>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring IP Routing on the Switch

The Cajun switch with integrated routing combines scalable wire speed IP layer 3 switching (routing) with 10/100/1000 Ethernet layer 2 switching (bridging) in a high-capacity chassis-based system.

For more detailed information on Cajun switch routing operations, see “Routing with Layer 2 and Layer 3 Modules”, in Chapter 1, *Introduction to the Cajun P550/P880/P882 Switch.*

Hardware Requirements for Routing

To configure your switch as an IP router, you must configure your Cajun switch with the following hardware:

- Layer 3 supervisor module
- Layer 3 media modules (optional) including:
  - 2-Port Gigabit Ethernet module
  - 10-Port 100-Base-F module
  - 12-Port 10/100-Base-T module

Minimum IP Routing Configuration Requirements

Your switch must be configured as follows to successfully create IP routing:

- IP routing must be globally enabled.
- At least one routing protocol (RIP, OSPF) must be enabled, if communication between routers is necessary.
- Interfaces that need to have IP routing enabled have been determined.
- VLANs (subnets) have been created to address your network configuration, if you plan to expand your current network.
- IP address, subnet mask, routing protocol, and multicast routing protocol to each IP interface that you configure have been assigned.

Routing Configuration Quickstart

This section provides an overview of the LAN router configuration operation. For more information on these configuration steps, see the sections referenced after each step.

To configure the switch as a LAN router:

1. Create an IP interface for each subnet. Refer to “Creating and Implementing VLANs”, in Chapter 4, Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping.
2. Create or assign a VLAN to the IP interface. Refer to “Configuring a Static Route for the PPP Console”, earlier in this chapter.
3. Bind ports to the VLANs assigned to the IP interfaces. Refer to “Viewing Switch Port Parameters”, in Chapter 5, Configuring Port Parameters.

4. Assign an IP address and subnet mask to the VLAN. Refer to "Configuring a Static Route for the PPP Console", earlier in this chapter.

5. Specify how the router will communicate with other routers. Refer to "Configuring a Static Route for the PPP Console", earlier in this chapter, to configure OSPF and RIP parameters.

Assigning IP Interfaces to the VLAN

After you have set up a VLAN and enabled IP Routing, you must create the IP interface that your VLAN and your subnet uses to communicate with each other. After creating the IP interface, you must assign it to the VLAN. If you need to create a new VLAN, refer to "Creating and Implementing VLANs in Chapter 4.

To create a new IP interface and assign it to a VLAN:

1. Select Interfaces from the Routing > IP > Configuration group on the web agent window. The IP Interfaces dialog box opens (Figure 9-1).

2. Refer to Table 9-1 to configure the IP interfaces dialog box parameters:

3. Click CREATE. The Add IP Interface dialog box opens (Figure 9-2).

4. Refer to Table 9-2 to configure the Add IP interface dialog box parameters.

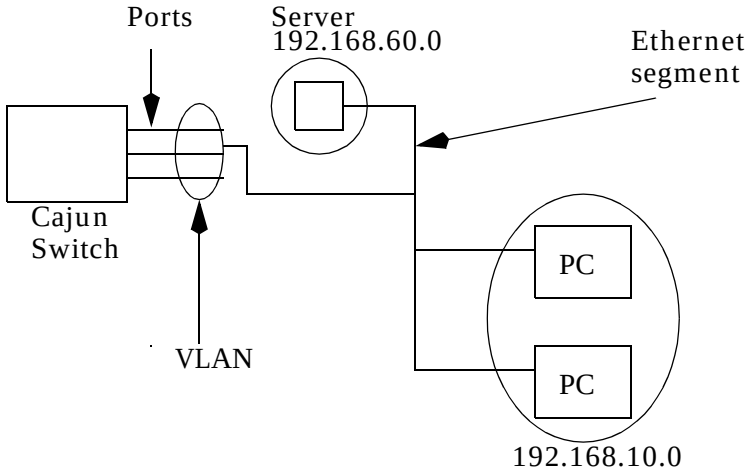
5. Click CREATE to save changes, or CANCEL to restore previous settings.

*** Note:** Routing is not supported on the serial interface. Do not configure Routing/Mgmt on serial IP interfaces.

IP Multinetting

You can set up a configuration of multiple subnets on a single VLAN, on the switches. This is also referred to as IP Multinetting. A network is said to be multinetted (Figure 9-4) when multiple logical groups of computers are brought together within a single broadcast domain. To create a multinetted network, you must assign multiple subnets to a VLAN.

Figure 9-4. Multinet Diagram



Creating a Multinet Interface

To create a multinet interface:

1. Select Interfaces from the Routing > IP > Configuration group on the web agent window. The IP Interfaces dialog box opens (Figure 9-1).
2. Select CREATE. The Add IP Interface dialog box opens (seeFigure 9-2).
3. Enter a name for the interface in the Interface field.
4. Select a VLAN for this multinet interface from the VLAN field pull-down menu.
5. Enter the network address associated with this interface in the Network Address field.
6. Select CREATE from the bottom of the Add IP Address dialog box. The IP Interfaces dialog box re-opens with the new interface name listed in the Interface field.
7. Repeat steps 2 through 6 for any other interfaces that you want to associate with the same VLAN.

*** Note:** You must have a different network address for each new multinetting interface that you create for the same VLAN.

Configuring Access Lists

Access Control Lists, also referred to as Access Lists, contain rules that forward or deny data to and through the switch. By configuring Access Lists, you can:

- Prioritize the transmission of frames within the switch.
- Filter out specific or general network transmissions (for example, all traffic from a particular subnet to the switch).

When you create an Access List, you create a series of rules that describe how data is forwarded or filtered within the switch. You can assign up to eight levels of priority to routed data.

Standard Access List support the conversion to the web agent of Cisco scripts that contain access lists. Extended access lists enable the switch to filter or deny information between two specified subnets via specific protocols, such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), and specified ranges of ports.

*** Note:** Access rules are searched in order of priority from first to last. During this search, the first rule that matches the frame is applied. If no rule is matched to a frame, then the frame is forwarded with normal priority. You cannot Access Lists to filter traffic destined to the switch's CPU. There is an implied **permit all** at the end of the list. Also, you can only have one list active at a time.

Creating Standard Access Rules

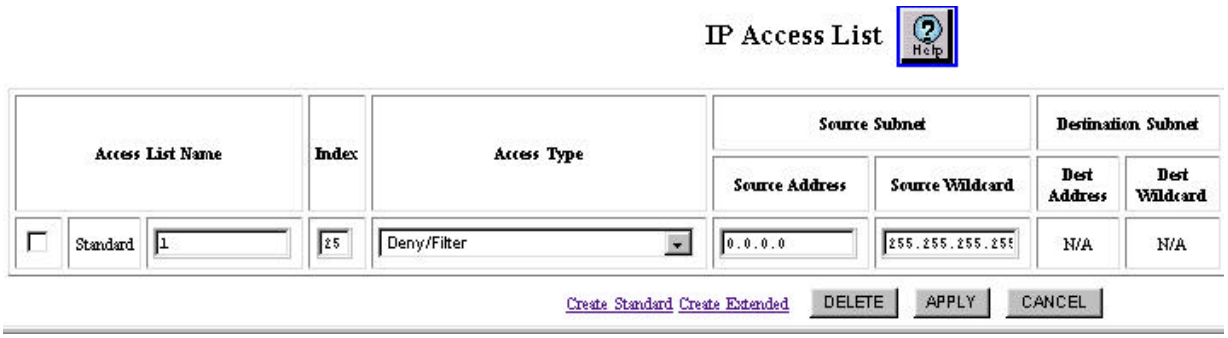
To create standard access rules:

1. Select Access Lists from the Routing > IP > Configuration group on the web agent window. The IP Access List dialog box opens (Figure 9-5).

   *** Note:** The IP Access List dialog box displays all standard and extended access rules that have been created. If no rules have been created, the following statement displays: `No IP Access Rules are currently configured`.

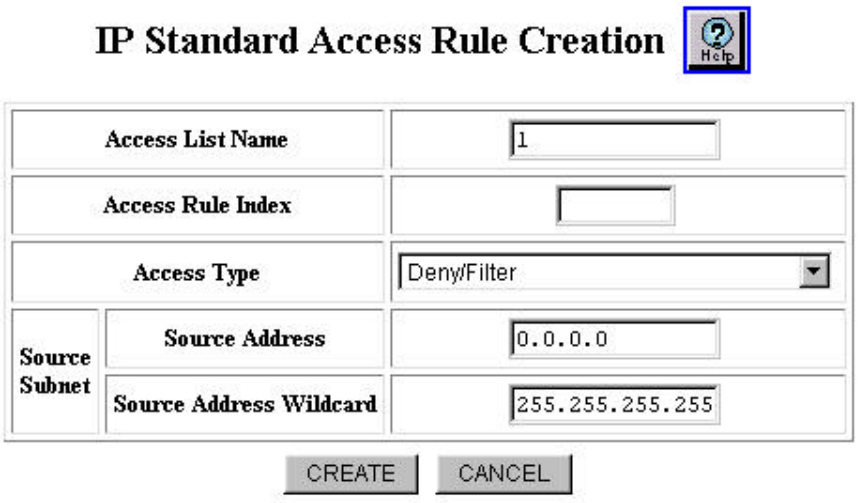
   *** Note:** Due to its size, Figure 9-5 shows the Access List dialog box split in two separate sections.

Figure 9-5. IP Access List Dialog Box



2. Select Create Standard. The Create Standard Access List dialog box opens (Figure 9-6).

Figure 9-6. Create IP Standard Access List Dialog Box



3. Refer to Table 9-4 to configure the Create Standard IP Access List dialog box to filter or prioritize traffic:

Table 9-4. Create Standard IP Access List Dialog Box Parameters

Parameter	Allows you to ...
Access List Name	Enter the alphanumeric name assigned to the newly-created access list.
Access Rule Index	Enter the sequence number for each new rule you create. **Note:** Entering a new rule may override other rules. Review your current configuration prior to creating new access list rules:
Access Type	Select the method of handling incoming datagrams based on the IP access type from the following pull-down menu options: • **Deny/Filter** - Allows you to filter out traffic based on the specified configuration. • **Permit/Fwd pri8 (high) to pri1 (low)** - Allows you to prioritize traffic based on the specified configuration. • **Permit/Fwd with no change in priority** - Allows you to forward traffic with no change in priority.
Source Subnet	• **Source Address** - Enter the IP address of a subnet that you want to deny or grant access to the switch. • **Source Address Wildcard** - Enter a range of IP addresses that you want to deny or grant access to the switch. Place the number one (1) in the bit positions for the IP addresses that you want to ignore.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating Extended Access Rules

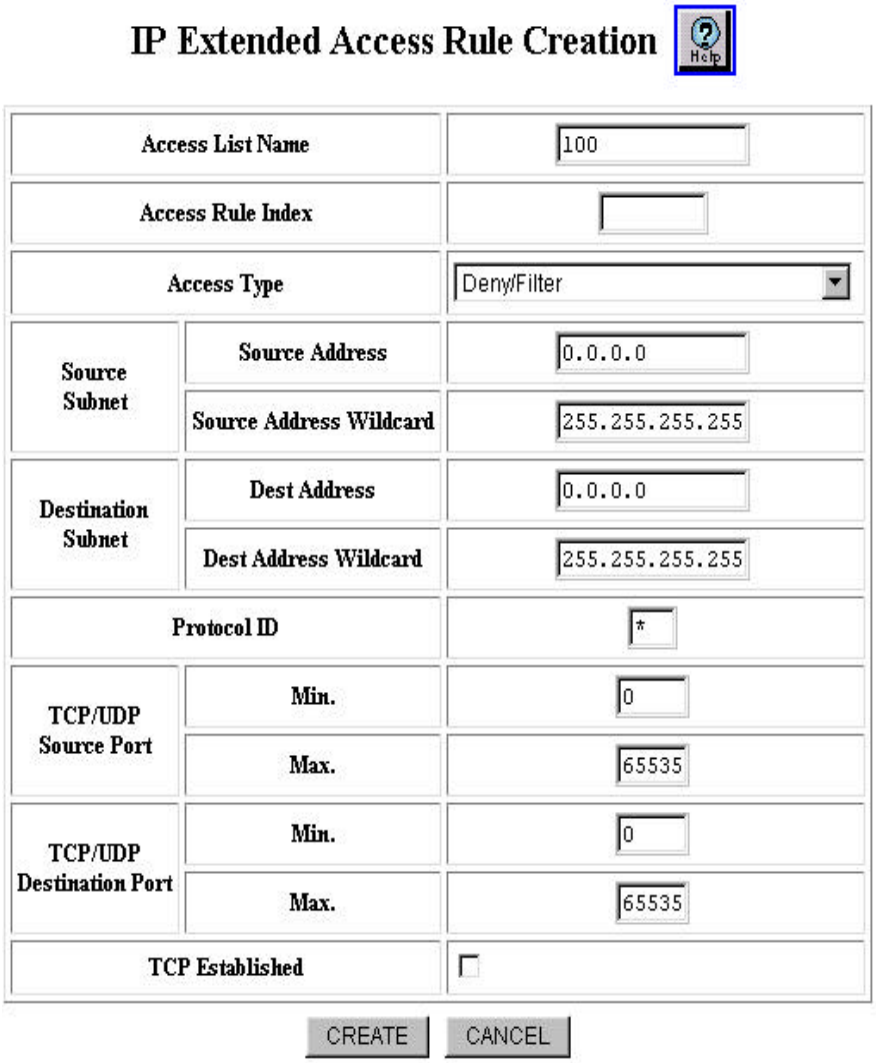
To create extended access rules:

1. Select Access Lists from the Routing > IP >Configuration group on the web agent window. The IP Access List dialog box opens (Figure 9-5).

   *** Note:** The IP Access List dialog box displays all standard and extended access rules that have been created. If no rules have been created, the following statement displays: `No IP Access Rules are currently configured`.

2. Select Create Extended. The IP Extended Access Rule Creation dialog box opens (Figure 9-7).

Figure 9-7. IP Extended Access Rule Creation Dialog Box



3. Refer to Table 9-5 to configure the IP Extended Access Rule Creation dialog box parameters to filter or prioritize traffic:

Table 9-5. IP Extended Access Rule Creation Parameters

Parameter	Allows you to...
Access List Name	Enter an alphanumeric name assigned to the newly-created access list.
Access Rule Index	Enter a sequence number for each new rule you create. Note that rules may override each other, so review your current configuration prior to creating new rules for an access list.

Table 9-5. IP Extended Access Rule Creation Parameters continued

Parameter	Allows you to...
Access Type	Select the method of handling incoming datagrams based on the IP access type you set from the following options: • **Deny/Filter** - Allows you to filter out traffic based on the specified configuration. • **Permit/Fwd pri8 (high) to pri1 (low)** - Allows you to prioritize traffic based on the specified configuration. • **Permit/Fwd with no change in priority** - Allows you to forward traffic with no change in priority.
Source Subnet	• **Source Address** - The IP address of a subnet that is denied or granted access to the switch. • **Source Address Wildcard** - A range of IP addresses that are denied or granted access to the switch. Place the number one (1) in the bit positions you want to ignore.
Destination Subnet	• **Dest Address** - The IP address of a subnet that is denied or granted access to data from the switch. • **Dest Address Wildcard** - A range of IP addresses of subnets that are denied or granted access to the switch. Place the number one (1) in the bit positions you want to ignore.
Protocol ID	Specify a protocol ID to be filtered. (For example, ICMP=1, IGMP=2). A single asterisk (*) indicates all protocols.
TCP/UDP Source Port	Specify a range of source ports that pass between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Options include: • **Min.** - The lowest numbered port in the range. The default is 0. • **Max.** - The highest numbered port in the range. The default is 65,535. To see the complete list of well-known port numbers (specifically in relation to the destination port), refer to the URL: http://www.isi.edu/in-notes/iana/assignments/port-numbers To see the complete list of protocol numbers, refer to the URL: http://www.isi.edu/in-notes/iana/assignments/protocol-numbers

***Table 9-5. IP Extended Access Rule Creation Parameters** continued*

Parameter	Allows you to...
TCP/UDP Destination Port	Specify a range of destination ports that pass data between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Options include: • **Min.** - The lowest numbered port in the range. The default is 0. • **Max.** - The highest numbered port in the range. The default is 65,535. To see the complete list of well-known port numbers (specifically in relation to the destination port), refer to the URL: http://www.isi.edu/in-notes/iana/assignments/port-numbers To see the complete list of protocol numbers, refer to the URL: http://www.isi.edu/in-notes/iana/assignments/protocol-numbers
TCP Established	Permit TCP connections to be established that match the rule. Non-established TCP connections will not match the rule.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Example: Filtering Web Traffic Using an Access Rule

To configure your switch to filter web traffic to or from a particular web server:

1. Select Access Lists from the Routing > IP > Configuration group on the web agent window. The IP Access List dialog box displays (Figure 9-5).
2. Select Create Extended. The IP Extended Access Rule Creation dialog box displays (Figure 9-7).
3. Enter a number between 100 and 199 in the Access List Name field to identify your new access control list.
4. Enter a number in the Access Rule Index field to identify the access rule.
5. Select Filter from the Access Type field pull-down menu.
6. Enter an * (asterisk) for the source address in the Source Address field.
7. Enter an IP address in the Dest Address field that represents the destination address of the web server.
8. Enter the following in the TCP/UDP Destination Port field:
   - a Min. of 0 (HTTP).
   - a Max. of 80 (HTTP).
9. Enter the following in the TCP/UDP Source Port field:
   - a Min. of 0 (HTTP).
   - a Max. of 80 (HTTP).
10. Select TCP Established. A check mark displays in the check box.
11. Click CREATE to save your changes, or CANCEL to restore previous settings.

Each time an end user attempts to access the corporate web server specified by the source and destination TCP/UDP ports, all web requests are filtered.

Example: Filtering Traffic Between Subnets

It is possible to filter traffic to either a specific address or to an entire subnet. In this example, all traffic between the two subnets is filtered:

- 10.1.1.0
- 10.1.2.0

This example also assumes that the network is a Class C network (255.255.255.0).

To filter traffic between both subnets, you must create two access rules.

To create the access rules:

1. Select Access Lists from the Routing > IP > Configuration group on the web Agent window. The IP Access List dialog box opens (Figure 9-5).
2. Select Create Extended. The IP Extended Access Rule Creation dialog box opens (Figure 9-7).
3. Enter a number between 100 and 199 in the Access List Name field to identify your new access control list.
4. Enter a number in the Access Rule Index file to identify the access rule.
5. Select Filter from the Access Type field pull-down menu.
6. Enter the source address (10.1.2.0) and the source address wildcard (0.0.0.255), respectively, in the Source Address field.
7. Enter the destination address (10.1.1.0) and the destination address wildcard (0.0.0.255), respectively, in the Dest Address field.
8. Enter the following in the TCP/UDP Destination Port field:
   - a Min. of 80(HTTP).
   - a Max. of 80 (HTTP).
9. Enter the following in the TCP/UDP Source Port field:
   - a Min. of 80(HTTP).
   - a Max. of 80 (HTTP).

10. Select TCP Established. A check mark displays in the check box.

11. Click CREATE to save your changes, or CANCEL to restore previous settings. Once you create both access rules, all traffic between subnet 10.1.1.0 and 10.1.2.0 is filtered.

*** Notes:** The traffic between subnet 10.1.1.0 and 10.1.3.0, and 10.1.2.0 and 10.1.3.0 is not filtered because the access rules only filter traffic between 10.1.1.0 and 10.1.2.0.

To filter traffic to a specific address and not to an entire subnet, you must specify the destination address of the network node, and use a subnet wildcard of 0.0.0.0.

To filter all traffic, you must specify a destination address of 0.0.0.0 and a subnet wildcard of 0.0.0.0. This is useful if you want to filter all traffic except traffic that matches a previous rule. Ensure that you *do not* make this your first rule, since that overrides all subsequent rules.

Activating Access Lists

You can activate access lists on the switch through the web agent and the CLI.

Activating Access Lists Using the Web Agent

To activate an access list using the web agent:

*** Note:** Before you can activate an access list, you must first configure the access lists. For information about configuring access lists, refer to "Configuring Access Lists" earlier in this chapter.

1. Select Access Control from the Routing > IP > Configuration group on the web agent. The IP Access Control dialog box opens (Figure 9-10).

Figure 9-8. IP Access Control Dialog Box

2. Select Enable from the Enable field pull-down menu to filter inbound traffic.
3. Select the name of the access list to be used for filtering when IP access control is enabled from the IP Access List field pull-down menu.
4. Click APPLY to save your changes, or CANCEL to restore previous settings.

Activating Access Lists Using the CLI

To activate an access list using the CLI, enter the following command in configure mode:

```
cajun (configure)# ip access-list <access-list-name> <access-list-index> {permit|deny|fwd[1-8]} {<source-ip-addr> [<source-wildcard>] |any|host <source-ip-addr>}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating IP Static Routes

You can create IP static routes using either the web agent or the CLI.

Creating IP Static Routes Using the Web Agent

To create IP static routes using the web agent:

1. Select Static Routes from the Routing > IP > Configuration group on the web agent window. The IP Static Routes dialog box opens (Figure 9-38).

2. Refer to Table 9-6 to configure the IP Static Route dialog box parameters:

Table 9-6. IP Static Route Parameters

Parameter	Allows you to...
Network Address	Enter an IP network address for your IP static route.
Mask	Enter an IP subnet mask for your IP static route.
Next-Hop Address	Enter an IP address for the gateway associated with the IP static route.
Next-Hop Interface	Enter an interface that is associated with the IP static route.
Cost	Enter the metric between this router and the destination. **Note:** The metric you enter overrides routing protocol metrics.
Preference	Select a *low* or *high* routing preference from the Preference field pull-down menu.

3. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating IP Static Routes Using the CLI

To create IP static routes using the CLI in configure mode:

```
cajun(configure)# ip route-preference <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating IP Static ARP Entries

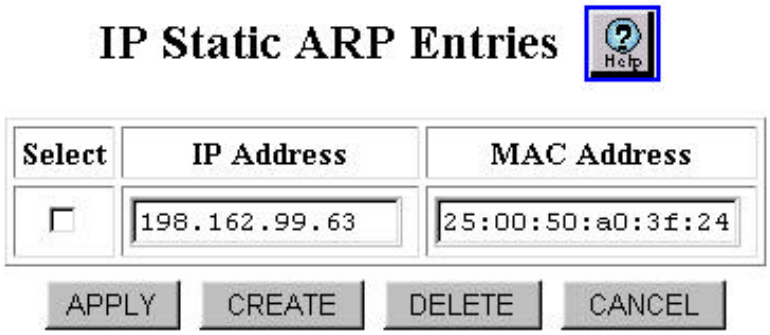
You can create static ARP entries on the switch using the web agent or the CLI.

Creating IP Static ARP Entries Using the Web Agent

To create a static ARP entry in your switch's ARP cache using the web agent:

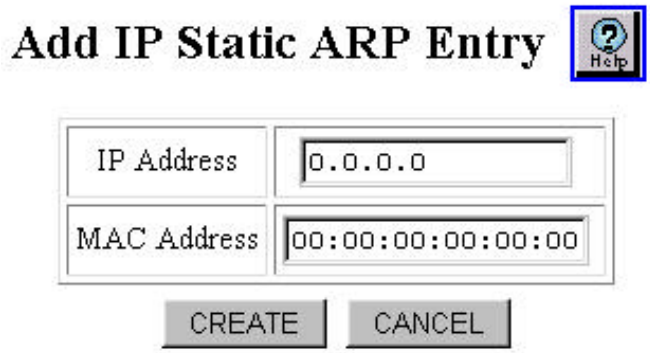
1. Select Static ARP from the Routing > IP > Configuration group on the web agent window. The IP Static ARP Entries dialog box opens (Figure 9-9).

Figure 9-9. IP Static ARP Entries Dialog Box



2. Select CREATE. The Add IP Static ARP Entry dialog box opens (Figure 9-12).

Figure 9-10. Add IP Static ARP Entry Dialog Box



3. Refer to Table 9-7 to configure the Add IP Static ARP Entry dialog box parameters:

Table 9-7. IP Static ARP Parameters

Parameter	Allows you to...
IP Address	Enter an IP address to associate with the Static ARP entry.
MAC Address	Enter the MAC address of a node to which you want to create a static ARP entry.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating IP Static ARP Entries Using the CLI

To create IP static ARP entries using the CLI, enter the following command in Configure mode:

```
Cajun(configure)# arp <ip-address> <hardware-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating a BOOTP/DHCP Server Entry

The BOOTP/DHCP Server Entry allows you to configure a Cajun Router as a BOOTP/DHCP Relay Agent between a BOOTP/DHCP server and the source client. Only the locally attached clients will be able to find the BOOTP/DHCP server if the BOOTP/DHCP server entry is configured on your switch. If you have a network with multiple switches, and you want at least one client that is attached to each switch to be able to access the BOOTP/DHCP server, then you must configure each of those switches with a BOOTP/DHCP server entry.

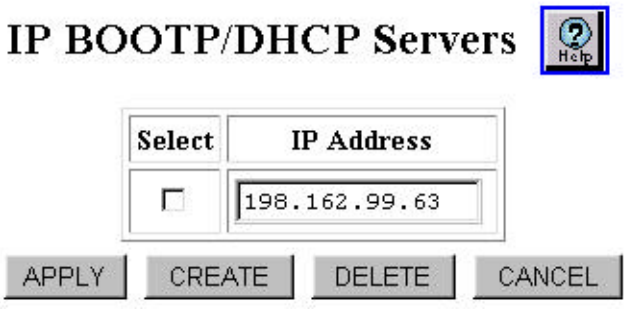
You can create a BOOTP/DHCP Server entry using wither the web agent or the CLI.

Creating a BOOTP/DHCP Server Entry Using the Web Agent

To create a BOOTP/DHCP entry using the web agent:

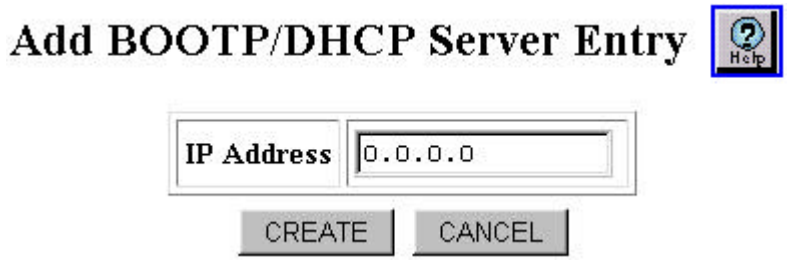
1. Select BOOTP/DHCP Servers from the Routing > IP > Configuration group on the web agent window. The IP BOOTP/DHCP Servers dialog box opens (seeFigure 9-11).

Figure 9-11. IP BOOTP/DHCP Server Dialog Box



2. Select CREATE. The Add BOOTP/DHCP Server Entry dialog box opens (Figure 9-14).

Figure 9-12. Add BOOTP/DHCP Server Entry Dialog Box



3. Enter the BOOTP/DHCP server IP address in the IP Address field.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

*** Note:** It is possible to create multiple BOOTP/DHCP Server Entries if necessary.

Creating a BOOTP/DHCP Server Entry Using the CLI

To create a BOOTP/DHCP entry using the CLI, enter the following command in Configure mode:

```
cajun (configure)# ip boot-dhcp server
<ip-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

IP Multicast

IP Multicast enables a single host to distribute information to multiple recipients. To do this, multicast protocols use class D IP addresses to specify specific multicast groups to which information is sent. The class D IP address used by multicast routing protocol ranges from 224.0.0.1 to 224.0.0.255. The class D IP addresses available for general use are 224.0.1.0 to 239.255.255.255.

In addition, IP multicasting distributes information to multicast groups in two specific ways:

- **Multicast Forwarding** - allows a switch to forward multicast traffic from the local router to group members on directly attached subnetworks. If a multicast packet is forwarded to multiple interfaces on one VLAN, only one Forwarding Entry is added on the VLAN for the packet. One copy of the packet is sent to the VLAN.
- **Multicast Routing** - allows a switch to deliver multicast traffic between neighboring routers and across the network.

For example, the switch could use Internet Group Management Protocol (IGMP) only to forward multicast traffic to locally attached subnetworks. However, if the multicast traffic in question is needed to be sent to a neighboring router, the switch could use DVMRP to send the information between routers. Since IGMP is a required protocol for any multicast routing protocol (for example, DVMRP), it is automatically enabled when you enable DVMRP.

*** Note:** You must globally enable IP multicast routing in order to successfully configure IGMP or DVMRP. Refer to "Configuring Internet Protocol (IP) Global Routing," earlier in this chapter, for instructions on enabling IP multicast routing.

Configuring IGMP

IGMP enables hosts to inform routers when they join or leave groups. Routers periodically query hosts (query interval) for the groups in which the hosts are members. When there is more than one router in a broadcast domain (subnet), one of the routers becomes the designated querier. Only the designated router queries the hosts.

Both IGMP Version 1.0 and IGMP Version 2.0 are supported. After selecting the specific IGMP version for an interface, you can manually configure the Version 1.0 querier. The selection of the querier for Version 2.0 is dynamic but can be overridden.

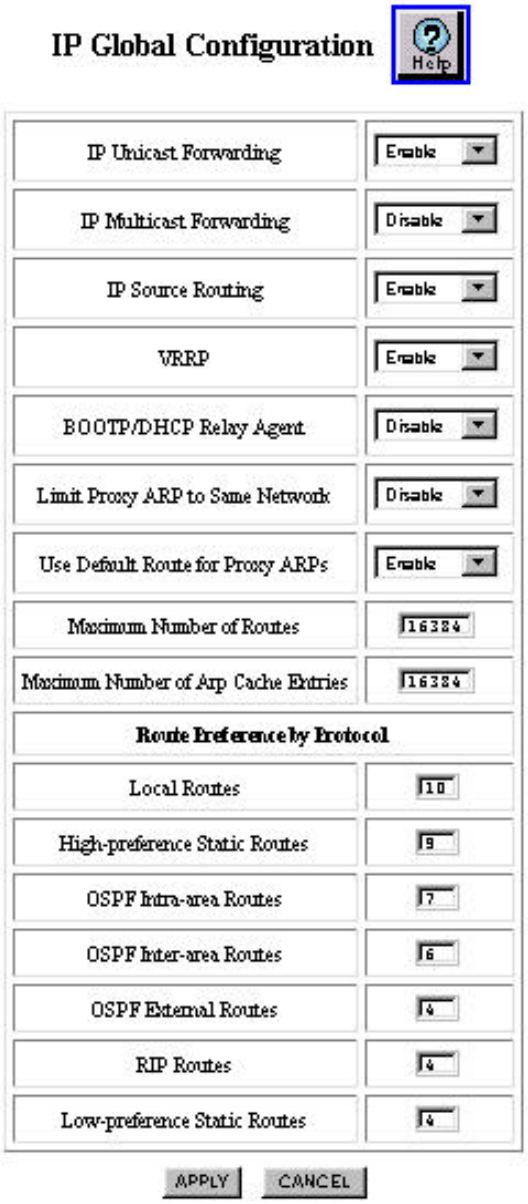
Configuring IGMP includes enabling IGMP and the MTRACE globally on the switch. You can do this from either the web agent or the CLI.

Globally Enabling IGMP Using the Web Agent

To globally enable IGMP from the web agent:

1. Select Global Configuration from the Routing > IP > Configuration group in the web agent window. The IP Global Configuration dialog box opens (Figure 9-15).

Figure 9-13. IP Global Configuration Dialog Box



2. Select Enable from the IP Multicast Forwarding field pull-down menu to enable IP multicast globally.

3. Select Global Configuration from the Routing > IGMP group on the web agent window. The IGMP Global Configuration dialog box opens (Figure 9-14).

Figure 9-14. IGMP Global Configuration Dialog Box

4. Select Enable from the IGMP field pull-down menu to enable IGMP.
5. Select Enable from the MTRACE field pull-down menu to enable MTRACE processing.
6. Click APPLY to save your changes, or CANCEL to restore previous settings.

Globally Enabling IGMP Using the CLI

To globally enable IGMP using the CLI, enter the following command from Configure mode:

```
cajun (configure)# set igmp-snooping enable
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

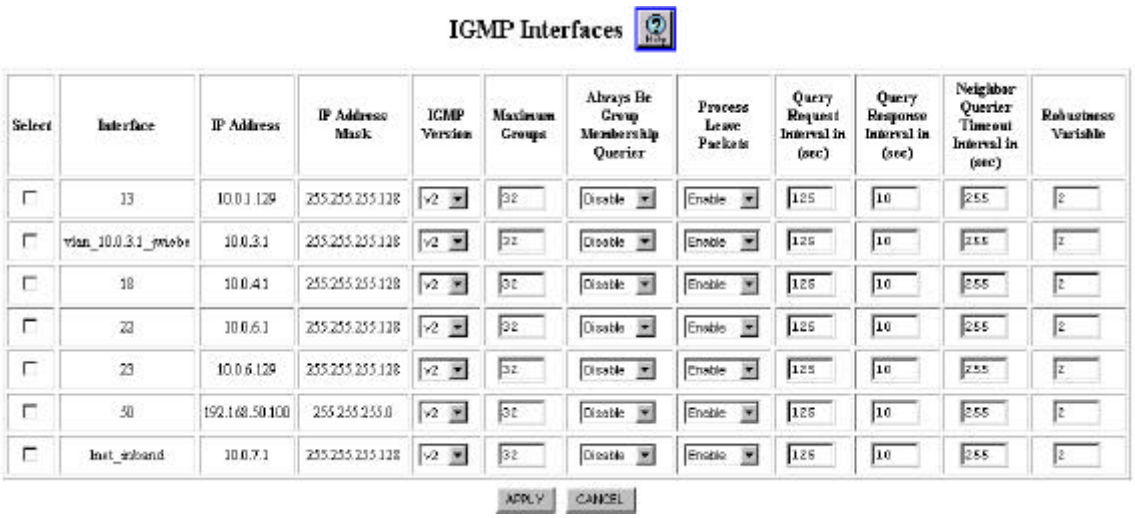
Modifying IGMP Interfaces Using the Web Agent

To modify IGMP interfaces from the web agent:

1. Select Interfaces from the Routing > IGMP group on the web agent window. The IGMP Interfaces dialog box opens (Figure 9-1).

*** Note:** You must first enable a multicast protocol before you can configure IGMP. Refer to *"Creating an IP Interface"* earlier in this chapter for more information on how to select a multicast protocol.

Figure 9-15. IGMP Interfaces Dialog Box



2. Refer to Table 9-8 to modify an IGMP interface:

Table 9-8. IGMP Interface Parameters

Parameter	Allows you to...
Select	Select the interface to be modified.
Interface	Displays the IP interface that is configured with IGMP.
IP Address	Displays the IP address associated with this interface. **Note:** This parameter is not configurable from the IGMP configuration dialog box.
IP Address Mask	Displays the subnet mask associated with this interface. **Note:** This parameter is not configurable from the IGMP configuration dialog box.
IGMP Version	Select the IGMP Version (1.0 or 2.0) to be associated with the IGMP interface.
Maximum Groups	Enter the number of IGMP Groups that can be active on this interface. The default value is 32.
Always be Group Membership Querier	**Version 1.0** - Select **Enable** to make this interface the designated querier. The default is **Disable**. **Version 2.0** - Select **Enable** to force this interface to send queries. The default is **Disable** which tells the interface to obey the designated querier election. **Note:** Only the designated router will query hosts on your network.

Table 9-8. IGMP Interface Parameters continued

Parameter	Allows you to...
Process Leave Packets	Select **Disable** to not terminate group memberships quickly (IGMP Version 2.0 only). The default value is **Enable**.
Query Request Interval in (sec)	Enter a time period between queries. The default value is **125** seconds.
Query Response Interval in (sec)	Enter a time (in seconds) to wait for a response from a host after a query is sent. If no response is received within this time, the host is removed from the group table. The default value is **10** seconds.
Neighbor Querier Timeout Interval in (sec)	Enter a time (in seconds) this interface should wait after hearing a neighbor's query before assuming the role of querier, if not already the querier. If no query is received from a neighbor with a lower IP address in the allotted time, this interface becomes the querier (IGMP Version 2.0 only). The default value is **255** seconds.
Robustness Variable	Modify this field for any expected packet loss on a subnet. If a subnet is expected to have more packet loss, the Robustness Variable should be increased. The Robustness Variable *must not* be set to 0 and *should not* be set to 1. The default value is **2**.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Modifying IGMP Interfaces Using the CLI

To modify an IGMP interface using the CLI, enter the following command from interface mode:

```
cajun(configure <interface-name>)# ip igmp
<options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring and Modifying Distance Vector Multicast Routing Protocol (DVMRP)

DVMRP uses IP packets with protocol type 2 (IGMP) to exchange routing datagrams. DVMRP enables multicast routers to exchange distance vector updates that contain multicast flow lists and their corresponding cost metrics. DVMRP uses tunneling between pairs of DVMRP routers when traffic must pass through one or more intermediary routers or gateways that do not implement DVMRP.

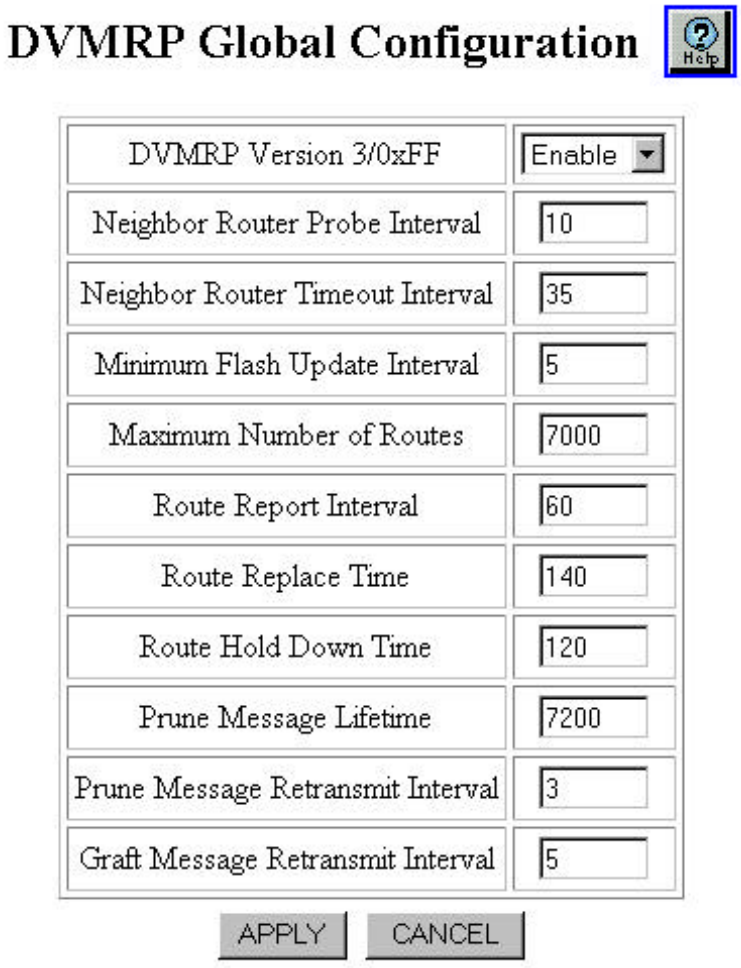
You can configure DVMRP Globally using either the web agent or the CLI.

Configuring the DVMRP Global Configuration Using the Web Agent

To configure DVMRP globally using the web agent:

1. Select Global Configuration from the Routing > IP > Configuration group on the web agent window. The IP Global Configuration dialog box opens (Figure 9-14).
2. Select Enable from the IP Multicast Forwarding field pull-down menu to enable IP multicast globally.
3. Select Global Configuration from the Routing > DVMRP group on the web agent window. The DVMRP Global Configuration dialog box opens (Figure 9-16).

Figure 9-16. DVMRP Global Configuration Dialog Box



4. Select Enable from the DVMRP Version 3/xFF field pull-down menu.

5. Refer to Table 9-9 to configure the DVMRP Global Configuration dialog box parameters:

Table 9-9. DVMRP Global Configuration Dialog Box Parameters

Parameter	Allows you to...
DVMRP Version 3/xFF	Select **Disable** to globally disable DVMRP. The default value is **Enable**.
Neighbor Router Probe Interval	Enter **probe interval** (in seconds) for the switch to probe the network for available neighbor routers.
Neighbor Router Timeout Interval	Enter the **time-out interval** (in seconds) that a neighbor stays up without confirmation. This is an important method used to time-out old routes.
Minimum Flash Update Interval	Enter the **update interval** (in seconds) between flash updates. This represents the minimum time between advertisements of the same route.
Maximum Number of Routes	Enter the maximum number of routes for this interface.
Route Report Interval	Enter the **report interval** (in seconds) that elapses between delivery of DVMRP routing table updates.
Route Replace Time	Enter the amount of **replace time** (in seconds) before which a route entry will be removed if it is not refreshed.
Route Hold Down Time	Set the **hold down time** (in seconds) that the switch reports unavailable routes with a metric of infinity.
Prune Message Lifetime	Enter the **lifetime** (in seconds) that a transmitted upstream prune message persists.
Prune Message Retransmit Interval	Enter the **retransmit interval** (in seconds) between the transmittal of generated upstream prune messages on your network.
Graft Message Retransmit Interval	Enter the **retransmit interval** (in seconds) between the transmittal of generated upstream graft messages.

6. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring the DVMRP Global Configuration Using the CLI

To configure DVMRP globally using the CLI:

```
cajun (configure <interface-name>)# ip dvmpr
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying a DVMRP Interface

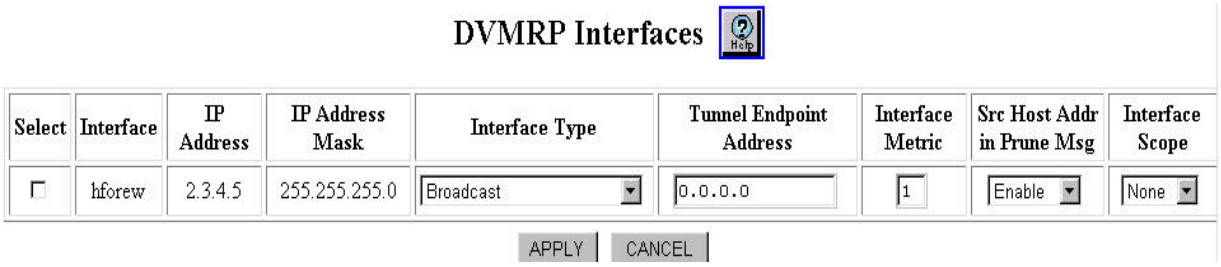
You can modify a DVMRP interface using either the web agent or the CLI.

Modifying the DVMRP Interface Using the Web Agent

To modify a DMVRP interface using the web agent:

1. Select Interfaces from the Routing > DVMRP group of the web agent window. The DVMRP Interfaces dialog box opens (see Figure 9-17).

Figure 9-17. DVMRP Interfaces Dialog Box



*** Note:** You must first enable a multicast protocol before you can configure DVMRP. Refer to *"Creating an IP Interface"*, earlier in this chapter, and enable a multicast protocol for this interface.

2. Refer to Table 9-10 to complete your DVMRP configuration:

Table 9-10. DVMRP Interface Parameters

Parameter	Defines the...
Select	Select a DVMRP interface that you want to configure.
Interface	Displays the Interface that is configured with the DVMRP multicast protocol.
IP Address	Displays the IP address of each interface. You cannot modify this field.
IP Address Mask	Displays the Subnet mask for each interface. You cannot modify this field.
Interface Type	Select an Interface type. You can configure the interface type as: • **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation. • **Non-Encapsulated Tunnel** - All multicast data traffic is IPIP encapsulated, but the protocol messages are unicast. • **IPIP Tunnel** - All multicast traffic (data and protocol messages) are encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP).
Tunnel Endpoint Address	Displays the Tunnel endpoint IP address of a router. You can modify this setting to represent the end router IP address to which you want to send datagrams through a tunnel. The origin and endpoint routers are separated by a gateway(s) or a router(s) that do not support DVMRP.
Interface Metric	Displays the Cost metric for the interface.
Src Host Addr in Prune Msg	Select **Disable to s**end prune messages with only the subnet portion of the source address. The default is **Enable (**sends prune messages with the full source host address).
Interface Scope	Select the minimum TTL (time-to-live) required for a packet to leave this interface. The options are None, 127, and 255.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Modifying the DVMRP Global Configuration Using the CLI

To configure the DVMRP global configuration using the CLI:

```
cajun (configure <interface-name>)# ip dvmrp
<options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Monitoring Switch Performance Using IP Statistics

This section provides detailed information on the analysis and use of IP and IP multicast statistics.

IP routing statistic options include:

- Displaying Global IP Routing Statistics Using the Web Agent
- Searching the IP Routing Table
- Displaying the IP Routing Table Statistics
- Searching the IP ARP Cache

Displaying Global IP Routing Statistics

You can monitor switch performance using either the web agent or the CLI.

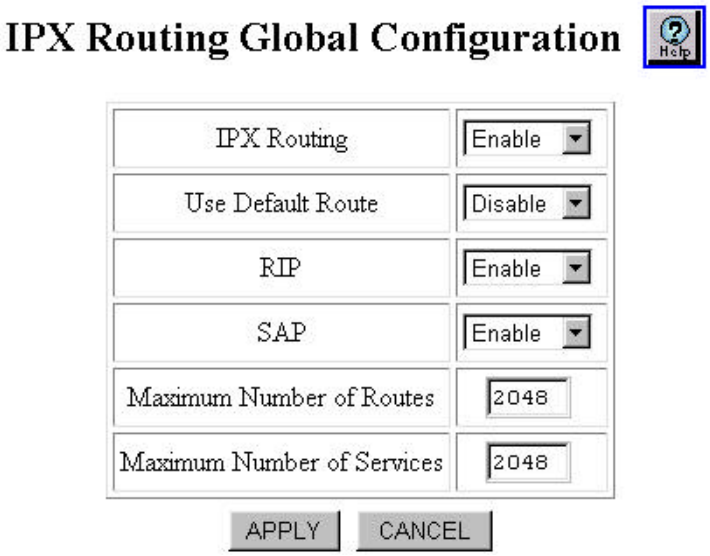
Displaying Global IP Routing Statistics Using the Web Agent

To display the global IP routing statistics using the web agent:

*** Note:** IP routing global statistics only represent traffic processed by the supervisor module software.

1. Select Global Statistics from the Routing > IP > Display group on the web agent window. The IP Routing Global Statistics dialog box opens (see Figure 9-18).

Figure 9-18. IP Routing Global Statistics Dialog Box



2. Click

   a. Clear to set all statistics to zero.

   b. Refresh to update all statistics.

3. Refer to Table 9-11 to review the definition of each statistic:

Table 9-11. IP Routing Global Statistics

Statistic	Defines the...
IP In Receives	Total number of input datagrams received from interfaces, including those received in error.
IP In Header Errors	Number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
IP In Address Errors	Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

***Table 9-11. IP Routing Global Statistics** continued*

Statistic	Defines the...
IP Forward Datagrams	Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful. **Note:** This is routed by the supervisor in the software.
IP In Unknown Protocols	Number of input datagrams discarded due to errors in their IP headers. Such errors may include bad checksums, version number mismatches, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
IP In Discards	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). **Note:** This counter does not include any datagrams discarded while awaiting re-assembly.
IP In Delivers	Total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IP Out Requests	Total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. **Note:** This counter does not include any datagrams counted in ipForwDatagrams.
IP Out Discards	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but were discarded (for example, for lack of buffer space). Note that this counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

Table 9-11. IP Routing Global Statistics continued

Statistic	Defines the...
IP Out No Routes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any Datagrams which a host cannot route because all of its default gateways are down.
IP Reassembly Timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
IP Reassembly Required	Number of IP fragments received that need to be reassembled.
IP Reassembly OKs	Number of IP datagrams successfully reassembled.
IP Reassembly Failures	Number of failures detected by the IP re-assembly algorithm (timeout errors). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IP Fragmentation OKs	Number of IP datagrams that have been successfully fragmented at this entity.
IP Fragmentation Failures	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be.
IP Fragmentation Creates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IP Routing Discards	Number of routing entries that were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ICMP In Messages	Total number of ICMP messages that the entity received. Note that this counter includes all those counted by icmpInErrors.
ICMP In Errors	Number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length).
ICMP In Destination Unreachables	Number of ICMP Destination Unreachable messages received.

Table 9-11. IP Routing Global Statistics continued

Statistic	Defines the...
ICMP In Time Exceeds	Number of ICMP Time Exceeded messages received.
ICMP In Parameter Problems	Number of ICMP Parameter Problem messages received.
ICMP In Source Quenchs	Number of ICMP Source Quench messages received.
ICMP In Redirects	Number of ICMP Redirect messages received.
ICMP In Echo Requests	Number of ICMP Echo (request) messages received.
ICMP In Echo Replies	Number of ICMP Echo Reply messages received.
ICMP In Timestamp Requests	Number of ICMP Timestamp (request) messages received.
ICMP In Timestamp Replies	Number of ICMP Timestamp Reply messages received.
ICMP In Address Mask Requests	Number of ICMP Address Mask Request messages received.
ICMP In Address Mask Replies	Number of ICMP Address Mask Reply messages received.
ICMP Out Messages	Total number of ICMP messages that this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMP Out Errors	Number of ICMP messages that this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations, there may be no types of error which contribute to this counter's value.
ICMP Out Destination Unreachables	Number of ICMP Destination Unreachable messages sent.
ICMP Out Time Exceeds	Number of ICMP Time Exceeded messages sent.
ICMP Out Parameter Problems	Number of ICMP Parameter Problem messages sent.
ICMP Out Source Quenchs	Number of ICMP Source Quench messages sent.
ICMP Out Redirects	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

Table 9-11. IP Routing Global Statistics continued

Statistic	Defines the...
ICMP Out Echo Requests	Number of ICMP Echo (request) messages sent.
ICMP Out Echo Replies	Number of ICMP Echo Reply messages sent.
ICMP Out Timestamp Requests	Number of ICMP Timestamp (request) messages sent.
ICMP Out Timestamp Replies	Number of ICMP Timestamp Reply messages sent.
ICMP Out Address Mask Requests	Number of ICMP Address Mask Request messages sent.
ICMP Out Address Mask Replies	Number of ICMP Address Mask Reply messages sent.
UDP In Datagrams	Total number of UDP datagrams delivered to User Datagram Protocol (UDP) users.
UDP In No Ports	Total number of received UDP datagrams for which there was no application at the destination port.
UDP In Errors	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
UDP Out Datagrams	Total number of UDP datagrams sent from this entity.
IP Multicast Forward Datagrams	Number of input multicast datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
IP Multicast In Discard	Number of input IP multicast datagrams for which no problems were encountered to prevent their continued processing, but were discarded (for example, for lack of buffer space). **Note:** This counter does not include any datagrams discarded while awaiting re-assembly.
IP Multicast In Receives	Total number of input multicast datagrams received from interfaces, including those received in error.
BOOTP/DHCP In Requests	Number of requests received by the BOOTP/DHCP Relay Agent.
BOOTP/DHCP In Responses	Total number of BOOTP/DHCP response datagrams received by the BOOTP/DHCP Relay Agent.

Table 9-11. IP Routing Global Statistics continued

Statistic	Defines the...
BOOTP/DHCP In Discards	Number of BOOTP/DHCP requests discarded.
BOOTP/DHCP In Hops Exceeds	Number of BOOTP/DHCP requests not forwarded due to number of hops exceeds.
BOOTP/DHCP Out Requests	Total number of BOOTP/DHCP requests forwarded by the BOOTP/DHCP Relay Agent.
BOOTP/DHCP Out Responses	Total number of BOOTP/DHCP responses forwarded by the BOOTP/DHCP Relay Agent.

Displaying Global IP Routing Statistics Using the CLI

To display the global IP routing statistics using the CLI, enter the following command from the prompt:

```
Cajun# show ip route summary
```

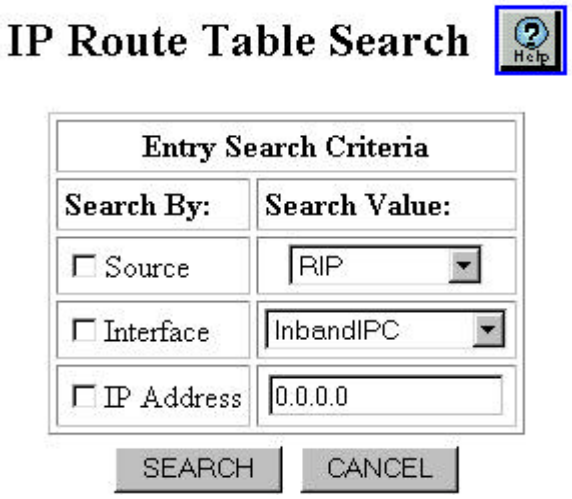
Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Searching the IP Routing Table

To use the IP routing table:

1. Select **Route Table Search** from the **Routing > IP > Display** group on the Web Agent window. The **IP Route Table Search** dialog box opens (Figure 9-19).

Figure 9-19. IP Route Table Search Dialog Box



2. Select the search criteria you want to use to find more specific information on available routes. For example, if you want to find all static routes that are presently configured on your switch, search by *source* and specify *static* as your search value.

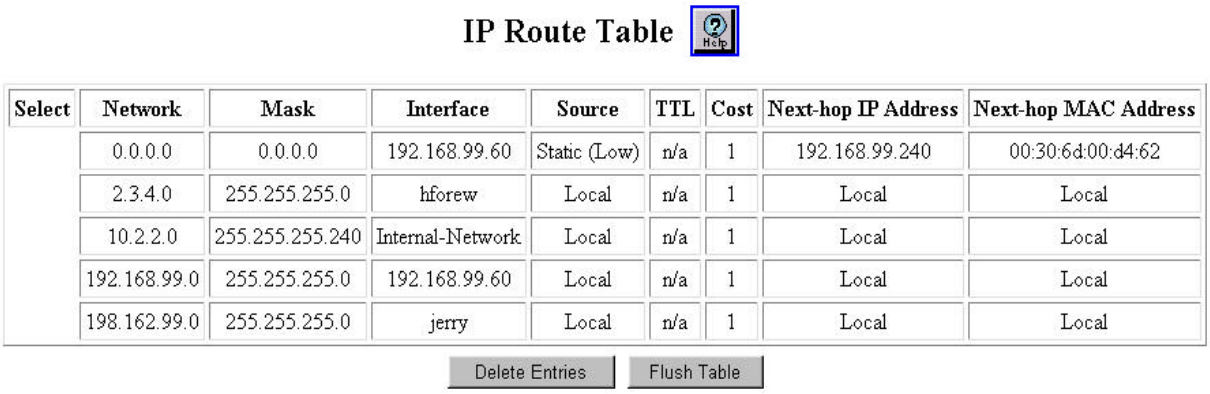
3. Refer to Table 9-12 to determine your search parameters:

Table 9-12. IP Route Table Search Parameters

Parameter	Allows you to search...
Source	Your IP routing table using one of the following parameters: • RIP • OSPF • Static • Local Once you select one of these parameters, the search attempts to find routes associated with that parameter.
Interface	The interface you selected. System default entries include: • **Default** • **Discard** • Ethernet Console • Configured Interface
IP Address	The IP address you entered.

4. Select SEARCH. If routes are available, they are displayed in the IP Routing Table dialog box (Figure 9-20).

Figure 9-20. IP Route Table Dialog Box



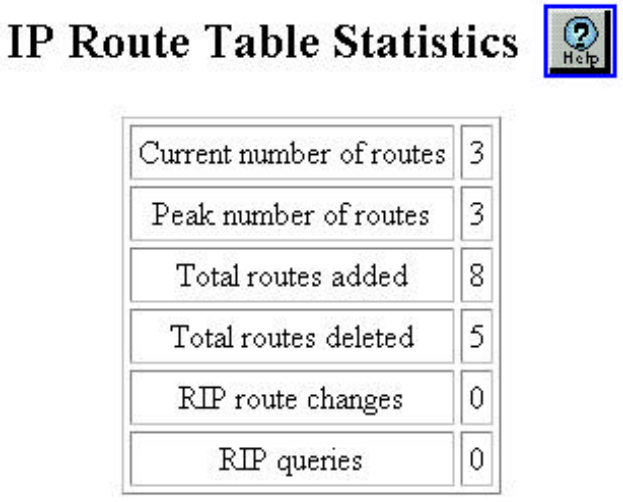
*** Note:** To delete a local entry from your IP routing table, you must delete the local IP interface associated with that entry.

Displaying the IP Routing Table Statistics

To display the IP Routing Table Statistics:

1. Select Route Table Statistics from the Routing > IP > Display group on the web agent window. The IP Routing Table Statistics dialog box opens (Figure 9-21)

Figure 9-21. IP Route Table Statistics Dialog Box



2. Refer to Table 9-13 for a definition of the IP Routing Table Statistical dialog box parameters:

Table 9-13. IP Routing Table Statistical Dialog Box Parameters

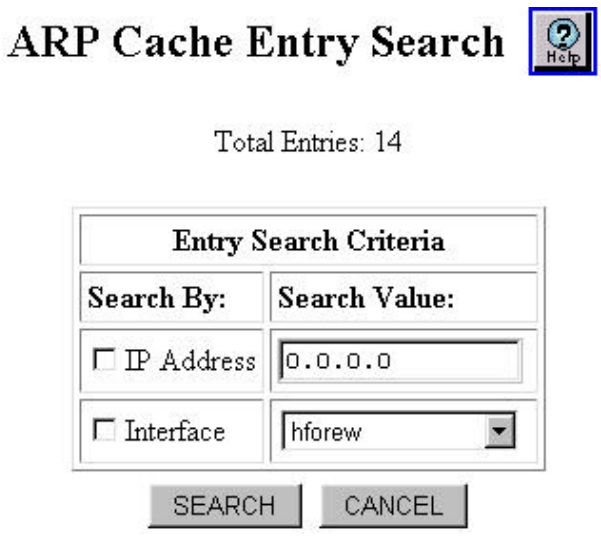
Parameter	Definition
Current Number of Routes	Displays the total number of active routes.
Peak Number of Routes	Displays the peak number of routes.
Total Routes Added	Displays the total number of routes added.
Total Routes Deleted	Displays the total number of routes deleted.
RIP Route Changes	Displays the number of changes to the IP route database made by RIP.
RIP Queries	Displays the number of RIP queries sent to the network.

Searching the IP ARP Cache

To search the IP ARP Cache entries:

1. Select ARP Cache Search from the Routing > IP > Display group on the Web Agent window. The ARP Cache Entry Search dialog box opens (Figure 9-22).

Figure 9-22. ARP Cache Entry Search Dialog Box



2. Select the search criteria you want to use to find more specific information on your switch's current ARP cache. For example, if you want to find all of the IP ARP cache entries associated with your out-of-band connection on your switch, search by **VLAN** and specify **Ethernet Console** as your search value.

3. Refer to Table 9-14 for an explanation of the ARP Cache Search dialog box parameters:

Table 9-14. ARP Cache Search Dialog Box Parameters

Parameter	Allows you to do a search based on...
IP Address	The IP address you entered.
Interface	The interface you selected. System entries include all interfaces that you previously configured.

4. Click SEARCH to start the search. If matching entries are found they are displayed in IP ARP Cache dialog box.

IP Multicast Statistics

You can view IP Multicast statistics through either the web agent or the CLI. IP multicast statistics include:

- Displaying IGMP Interface Statistics
- Displaying IGMP Interface Statistics Using the CLI
- Displaying the IGMP Local Multicast Forwarding Cache
- Displaying DVMRP Global Statistics
- Displaying DVMRP Interface Statistics
- Displaying DVMRP Neighbor Router(s)
- Displaying DVMRP Routing Table Statistics
- Displaying the DVMRP Route Table
- Displaying the DVMRP Upstream Routers
- Displaying the DVMRP Designated Forwarder(s) Table
- Displaying the DVMRP Downstream Dependent Router(s)
- Displaying the DVMRP Multicast Forwarding Cache

*** Note:** It is possible to use **access rules** to filter and prioritize multicast traffic.

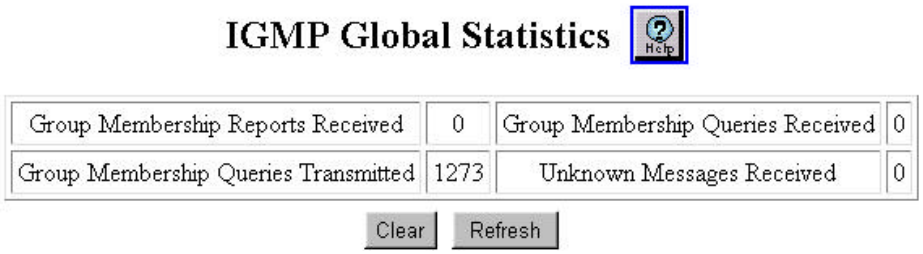
Displaying IGMP Global Statistics Using the Web Agent

IGMP global statistics provides membership reports, membership queries transmitted and received, and unknown messages.

To display IGMP global statistics from the web agent:

1. Select Global Statistics from the Routing > IGMP group on the web agent window. The IGMP Global Statistics dialog box opens (Figure 9-23).

Figure 9-23. IGMP Global Statistics Dialog Box



2. To modify your global statistics, perform one of the following:
   - Click CLEAR to reset all statistics to zero
   - Click REFRESH to view the latest statistics.
3. Refer to Table 9-15 for an explanation of the IGMP Global Statistics dialog box parameters:

Table 9-15. IGMP Global Statistics Dialog Box Parameters

Parameter	Defines the...
Group Membership Reports Received	Number of reports received in response to a group membership query. Hosts respond to a Query by generating Host Membership Reports reporting each host group to which they belong on the network interface from which the Query was received.
Group Membership Queries Transmitted	Number of query messages sent by all local IGMP interfaces. These messages are sent to discover which host groups have members on their attached local networks. Queries are addressed to the all-hosts group (address 224.0.0.1), and carry an IP time-to-live of 1.
Group Membership Queries Received	Number of query messages received by all local IGMP interfaces. All hosts that receive this query transmit a group membership report reporting each host group to which they belong.
Unknown Messages Received	IGMP message of a type *other* than Group Membership Query, Group Membership Report, or Leave group.

Displaying IGMP Global Statistics Using the CLI

To view IGMP Global Statistics using the CLI, enter the following command in **enable** mode:

```
cajun# show igmp-snooping statistics
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying IGMP Interface Statistics

You can examine IGMP interface statistics for each configured IP interface with multicast enabled through the **IGMP Interface Statistics** window.

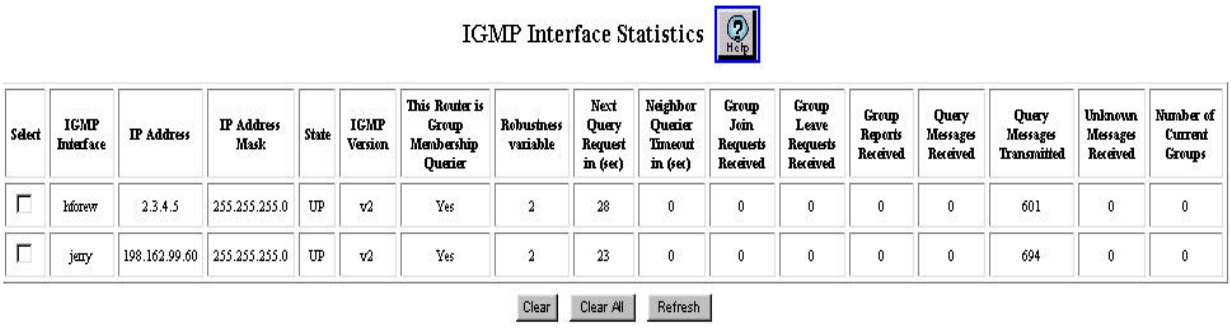
You can display IGMP interface statistics using either the web agent or the CLI.

Displaying IGMP Interface Statistics Using the Web Agent

To display the IGMP Interface Statistics window using the web agent:

1. Select Interface Statistics from the Routing > IGMP > group on the web agent window. The IGMP Interface Statistics dialog box opens (Figure 9-24).

Figure 9-24. IGMP Interface Statistics Dialog Box



2. To modify the interface statistics, perform one of the following:

   — Select one or more interfaces, and click CLEAR to reset statistics on those interfaces to zero.

   — Click CLEAR ALL to reset all statistics to zero.

   — Click REFRESH to view the latest interface statistics.

3. Refer to Table 9-16 fro an explanation of the IGMP Interface Statistics dialog box parameters:

Table 9-16. IGMP Interface Statistical Dialog Box Parameters

Parameter	Defines the...
IGMP Interface	IP interface for these statistics.
IP Address	IP address associated with the interface.
IP Address Mask	Subnet mask associated with each listed interface.
State	Current state of the interface. For example, if the interface is enabled and operating properly, UP is displayed.
IGMP Version	Version of IGMP enabled on each interface.
This Router is Group Membership Querier	Router that was configured or elected to be the designated **group membership querier**. The switch queries hosts on each interface only when it is acting as the designated querier on that interface.
Robustness Variable	Setting for the expected packet loss on a subnet. If a subnet is expected to have more packet loss, the Robustness Variable should be increased. The Robustness Variable must not be set to 0 and should not be set to 1.
Next Query Request (sec)	Remaining amount of time (in seconds) before the next group membership query is transmitted.
Neighbor Querier Timeout (sec)	Amount of time (in seconds) remaining before this interface assumes the role of designated querier. This timer is reset to the value entered for the Neighbor Querier Timeout Interval each time an IGMP query is received from a neighbor with a lower IP address. If no response is received in the allotted time, the query will timeout and the Version 2.0 querier will begin.
Group Join Requests Received	Number of new groups on this interface.
Group Leave Requests Received	Number of leave requests received on this interface.
Group Reports Received	Number of reports received on this interface in response to a group membership query. Hosts respond to a Query by generating Host Membership Reports reporting each host group to which they belong on the network interface from which the Query was received.
Query Messages Received	Number of query messages received from other multicast routers.
Query Messages Transmitted	Number of query messages sent by a multicast router. These messages are sent to discover which host groups have members on their attached local networks. Queries are addressed to the all-hosts group (address 224.0.0.1), and carry an IP time-to-live of 1.

Table 9-16. IGMP Interface Statistical Dialog Box Parameters continued

Parameter	Defines the...
Unknown Messages Received	IGMP messages received with an unsupported type.
Number of Current Groups	Number of groups on each interface for which there are entries in the Group Membership Table.

Displaying IGMP Interface Statistics Using the CLI

To display the IGMP Interface Statistics window using the CLI, enter the following command from User mode:

```
cajun> show ip igmp statistics
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying the Multicast Group Table

The multicast group table provides information on interfaces that are members of an IGMP group and contains an expiry time for the entry, IP address of the group, and the group reporter address.

To display the multicast group table:

1. Select Group Membership Table from the Routing > IGMP group on the web agent window. The IGMP Group Membership Table dialog box opens.
2. To modify the IGMP Group Membership Table, perform one of the following:
   - Select the entry and click Delete Entry to delete one or more entries.
   - Click Flush Table to clear the entire table.
   - Click REFRESH to receive the most up-to-date information on the entries in the table.

3. Refer to Table 9-17 for an definition of the IGMP Group Membership information dialog box parameters:

Table 9-17. IGMP Group Membership Table Dialog Box Parameters

Parameter	Defines the...
Group Member Interface	Interface that is connected to a member of an IGMP group.
Group Address	Group address that has members on this interface.
Group Created On	Time at which the group was created on the router.
Group Multicast Protocol	Routing protocol being used for the group. If no routing protocol is being used on the interface a group is on, this column displays IGMP.
Group Reporter Address	IP address of the host that sent the most recent host membership report for this group.
Entry Expiration Period in (sec)	Expiration time (in seconds) of the group that is being displayed.

Displaying the IGMP Local Multicast Forwarding Cache

To display the multicast forwarding cache information (IGMP only interfaces):

1. Select Local Multicast Forwarding Cache from the Routing > IGMP group on the web agent window. The Local Multicast Forwarding Cache dialog box opens.

2. To modify the Local Multicast Forwarding Cache, select an entry and:

   — Click Delete Entry to delete one or more entries.

   — Click Flush Table to clear the entire table.

   — Click REFRESH to receive the most up-to-date information on the entries in the table.

3. Refer to Table 9-18 to review the IGMP Multicast Forwarding Cache information:

Table 9-18. IGMP Local Multicast Forwarding Cache Parameters

Parameters	Defines the...
Destination Group Address	Destination group address of the multicast transmission.
Source SubNetwork	Subnet on which the IGMP interface(s) exist.
Source Address Mask	Subnet mask associated with the IGMP source subnetwork.
Upstream Interface	IP interface configured on the upstream interface.
Invalid Flows From Upstream	Number of invalid flows received from the upstream neighbor.
Packets Forwarded Through Cache Entry	Number of packets successfully forwarded in the CPU (supervisor module).
Downstream Interface(s)	Number of downstream interfaces and provides a link to the IGMP Downstream Interfaces dialog box.
Upstream Source(s)	Number of upstream interfaces and provides a link to the IGMP Upstream Interfaces dialog box.

Displaying DVMRP Global Statistics

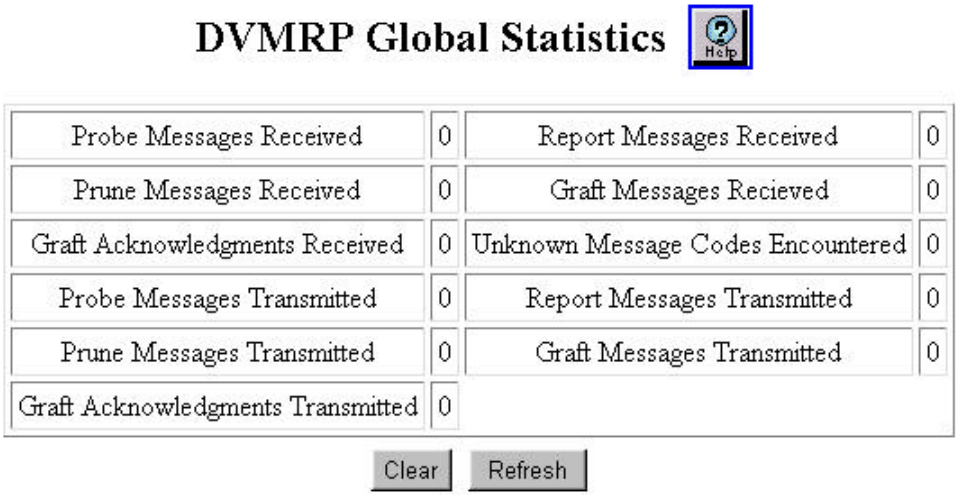
You can view the DVMRP Global Statistics from either the web agent or the CLI.

Displaying DVMRP Global Statistics Using the Web Agent

To display the DVMRP global statistics:

1. Select **Global Statistics** from the **Routing > DVMRP** group on the web agent window. The **DVMRP Global Statistics** dialog box opens (Figure 9-25).

Figure 9-25. DVMRP Global Statistics Dialog Box



2. Click:
   - CLEAR to reset all statistics to zero
   - REFRESH to view the latest statistics.
3. Refer to Table 9-19 for an explanation of the DVMRP Global Statistics dialog box parameters:

Table 9-19. DVMRP Global Statistics Dialog Box Parameters

Statistic	Defines the number of...
Probe Messages Received	Probe messages received on this switch. DVMRP routers exchange probes and routing updates so they each have a picture of their neighbors' capabilities and the DVMRP network topology.
Report Messages Received	Report messages received on this switch.
Prune Messages Received	Prune messages received on this switch. This indicates the number of old branches removed from the multicast distribution tree.
Graft Messages Received	Graft messages received. This indicates the number of attempts at adding a new branch to the multicast distribution tree.
Graft Acknowledgments Received	Graft acknowledgments received.
Unknown Message Codes Encountered	Messages received that are not graft, report, or probe messages.
Probe Messages Transmitted	Probe messages transmitted to the network.

Table 9-19. DVMRP Global Statistics Dialog Box Parameters continued

Statistic	Defines the number of...
Report Messages Transmitted	Report messages transmitted on this switch.
Prune Messages Transmitted	Prune messages transmitted upstream on this switch. This indicates the number of old branches removed from the multicast distribution tree.
Graft Messages Transmitted	Graft messages transmitted upstream from this switch. This indicates the number of new upstream branches added to the multicast distribution tree.
Graft Acknowledgments Transmitted	Graft acknowledgments sent downstream from this switch. This indicates the number of new downstream branches added to the multicast distribution tree.

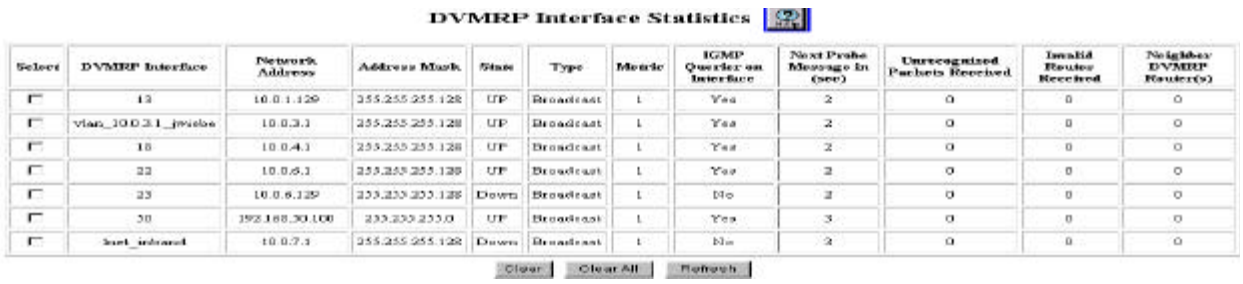
Displaying DVMRP Interface Statistics

DVMRP interface statistics list active DVMRP interfaces and provide specific information on each interface.

To display DVMRP interface statistics:

1. Select Interface Statistics from the Routing > DVMRP group on the web agent window. The DVMRP Interface Statistics dialog box opens (Figure 9-26).

Figure 9-26. DVMRP Interface Statistics Dialog Box


DVMRP Interface Statistics
Select
DVMRP Interface
Network Address
Address Mask
State
Type
Metric
IGMP Querier on Interface
Next Probe Message in (sec)
Unrecognized Packets Received
Invalid Router Received
Neighbor DVMRP Router(s)
13 10.0.1.129 255.255.255.128 UP Broadcast 1 Yes 2 0 0 0
vlan_10.0.3.1_jvielse 10.0.3.1 255.255.255.128 UP Broadcast 1 Yes 2 0 0 0
18 10.0.4.1 255.255.255.128 UP Broadcast 1 Yes 2 0 0 0
22 10.0.6.1 255.255.255.128 UP Broadcast 1 Yes 2 0 0 0
23 10.0.6.129 255.255.255.128 Down Broadcast 1 No 2 0 0 0
50 192.168.50.100 255.255.255.0 UP Broadcast 1 Yes 3 0 0 0
test_inbrand 10.0.7.1 255.255.255.128 Down Broadcast 1 No 2 0 0 0
Clear
Clear All
Refresh

2. Select an interface an perform one of the following:
   - Click REFRESH to view the latest interface statistics.
   - Click CLEAR All to reset all statistics to zero.
   - Click CLEAR to reset the selected interface.

3. Refer to Table 9-20 for an explanation of the DVMRP Interface Statistics dialog box parameters:

Table 9-20. DVMRP Interface Statistics Parameters

Parameter	Defines the ...
DVMRP Interface	IP interface configured with the DVMRP multicast routing protocol.
Network Address	IP address of the interface configured with the DVMRP multicast.
Address Mask	IP subnet mask associated with the interface.
State	Current status of the interface. Possible status indications include: • **UP** - The interface is active. • **DOWN** - The interface is inactive.
Type	Type of interface configured. Possible values include: • **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation. • **IPIP Tunnel** - All multicast traffic (data and protocol messages) on this interface is encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP). • **Non-Encapsulated Tunnel** - All multicast data traffic on this interface is IPIP encapsulated, but the protocol messages are simple unicast.
Metric	Interface cost.
IGMP Querier on Interface	Router is the IGMP querier. The purpose of the IGMP querier is to periodically poll hosts on your network to trigger group membership reports.
Next Probe Message in (sec)	Time (in seconds) remaining until the next probe message is sent.
Unrecognized Packets Received	Number of unknown DVMRP messages.
Invalid Routes Received	Number of invalid routes received on this interface.
Neighbor DVMRP Router(s)	Number of (neighbor) routers that are also running DVMRP. **Note:** This number is a hypertext link that provides additional information on the DVMRP neighbor router(s).

Displaying DVMRP Neighbor Router(s)

To view the DVMRP neighbor routers:

1. Select Interface Statistics from the Routing > DVMRP group on the web agent window. The DVMRP Interface Statistics dialog box opens (Figure 9-26).
2. Select the number in the Neighbor DVMRP Router(s) column, if it is 1 or more. The DVMRP neighbor routers dialog box opens.
3. Refer to Table 9-21 to view more information on DVMRP neighbor routers.

Table 9-21. DVMRP Neighbor Routers

Parameter	Displays...
Neighbor Network Address	The neighbor router's network address.
Found on Interface	The neighbor routers found on this interface.
DVMRP Supported Major/ Minor Version	The DVMRP version supported by the neighbor router.
Expiration period in (sec)	The time (in seconds) before the neighbor router times out.
Neighbor Received Probe From This Router	Whether the neighbor router received this router's probe message.
Neighbor Supports Prune Function	Whether the neighbor router supports prune functionality.
Neighbor Supports Generation ID Function	Whether the neighbor router supports generation of IDs.
Neighbor Supports MTRACE Requests	Whether the neighbor router supports MTRACE requests.
Neighbor is SNMP Manageable	Whether the neighbor router can be managed by SNMP.

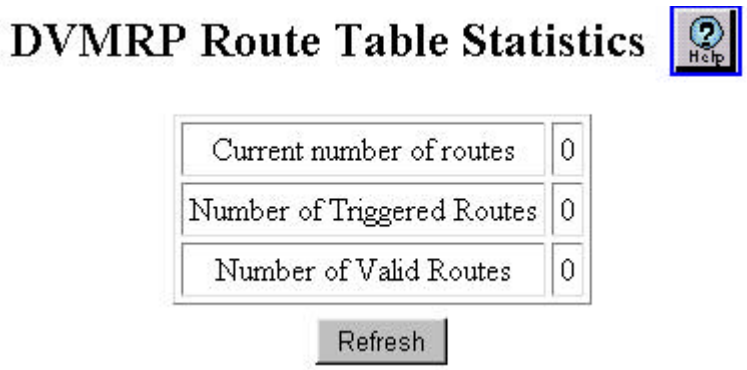
Displaying DVMRP Routing Table Statistics

DVMRP routing table statistics provides information on the current number of valid routes, the number of total routes present (both valid and invalid), and the number of triggered routes.

To view the DVMRP routing table statistics:

1. Select Route Table Statistics from the Routing > DVMRP group on the web agent window. The DVMRP Routing Table Statistics dialog box opens (Figure 9-27).

Figure 9-27. DVMRP Route Table Statistics Dialog Box



2. Refer to Table 9-22 for an explanation of the DVMRP Route Table Statistics dialog box parameters:

Table 9-22. DVMRP Routing Statistical Parameters

Parameter	Defines the...
Current Number of Routes	Total number of routes present in the routing database. This number includes both valid and invalid routes.
Number of Triggered Routes	Total number of routes added to the routing table that were triggered by a topology change in the network.
Number of Valid Routes	Total number of *valid routes* present in the routing database.

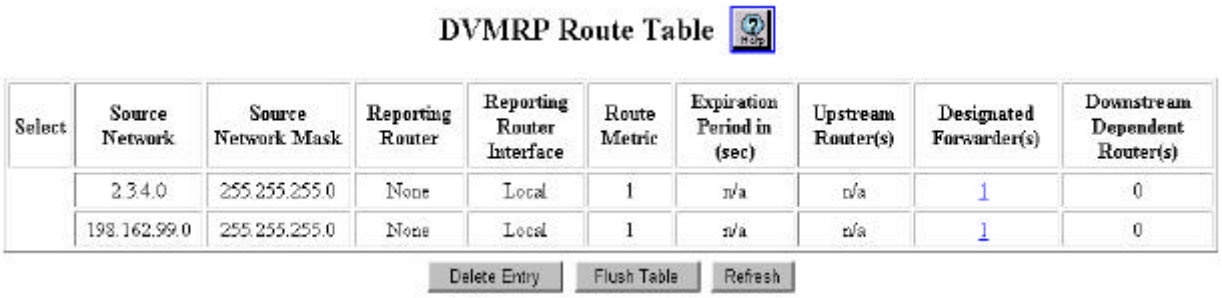
Displaying the DVMRP Route Table

The DVMRP route table contains information on valid DVMRP routes, the expiry for those routes, and additional next-hop information.

To view the DVMRP route table:

1. Select Route Table from the Routing > DVMRP group on the web agent window. The DVMRP Route Table dialog box opens (Figure 9-28).

Figure 9-28. DVMRP Route Table Dialog Box



2. To modify your DVMRP Route table, do one of the following:
   - Select the entry and click Delete Entry *to* delete one or more entries.
   - Click Flush Table *to clear the entire table*.
   - Click REFRESH to receive the most up-to-date information on the entries in the table.
3. Refer to Table 9-23for an explanation of the DVMRP Route table parameters:

Table 9-23. DVMRP Route Table Parameters

Parameter	Defines the...
Source Network	Network from which a multicast flow may originate.
Source Network Mask	Source network mask.
Reporting Router	IP address of the router reporting this route to its neighbors.
Reporting Router Interface	IP interface configured, which leads to the upstream neighbor (DVMRP router).
Route Metric	Router's cost to source network.
Expiration Period in (sec)	Time (in seconds) remaining before the source network is removed from the DVMRP routing table.

Table 9-23. DVMRP Route Table Parameters continued

Parameter	Defines the...
Upstream Router(s)	IP address of the DVMRP router that is the upstream neighbor to the local router. The local DVMRP router must know which DVMRP router is its upstream neighbor to determine how packets from a given source will be transmitted to a given multicast group. Opens DVMRP Upstream Router(s) dialog box.
Designated Forwarder(s)	Network router(s) responsible for forwarding from the source network onto the upstream interface. Opens the Designated Forwarders dialog box.
Downstream Dependent Router(s)	Number of downstream DVMRP routers that are dependent on this router for this particular route. Opens the DVMRP Downstream Dependent Router(s) dialog box.

Displaying the DVMRP Upstream Routers

To view the DVMRP upstream routers:

1. Select Route Table from the Routing > DVMRP group on the web agent window, The DVMRP Route Table dialog box opens (Figure 9-28).
2. Select the number in the Upstream Router(s) column to view information on the upstream routers. The Upstream Router(s) dialog box opens.
3. Refer to Table 9-24 for an explanation of the DVMRP Upstream Router(s) dialog box parameters.

Table 9-24. DVMRP Upstream Router(s) Dialog Box Parameters

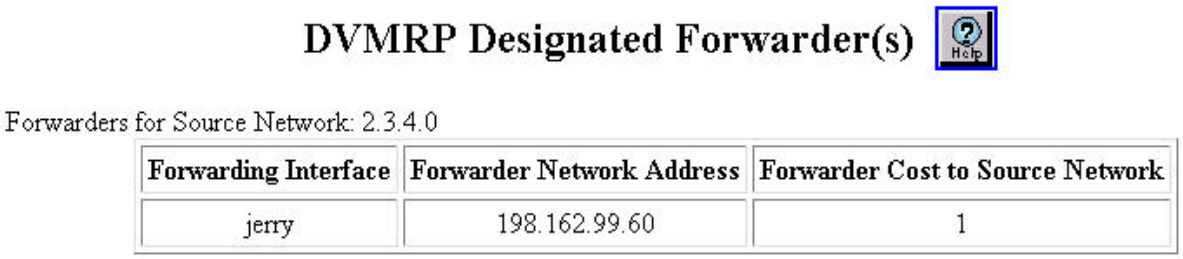
Parameter	Definition
Router Network Address	Displays the router network address.
Router Cost to Source Network	Displays the cost metric.
Found on Interface	Displays the interface on which the upstream router was found.

Displaying the DVMRP Designated Forwarder(s) Table

To view the DVMRP Designated Forwarder table:

1. Select Route Table from the Routing > DVMRP group on the web agent window. The DVMRP Route Table dialog box opens (see Figure 9-28).
2. Select the number from the Designated Forwarder column for the appropriate source network. The Designated Forwarder(s) Table dialog box opens (see Figure 9-29).

Figure 9-29. Designated Forwarder(s) Table Dialog Box



3. Refer to Table 9-25 for an explanation of the DVMRP Designated Forwarder(s) dialog box parameters:

Table 9-25. DVMRP Designated Forwarder(s) Table Dialog Box Parameters

Parameter	Defines the...
Forwarding Interface	Local interface which leads to the network where the Designated Forwarder resides.
Forwarder Network Address	Designated Forwarder for the given source network on the indicated Forwarding Interface.
Forwarder Cost to Source Network	Cost reported by the Designated Forwarder for the given source network.

Displaying the DVMRP Downstream Dependent Router(s)

To view the DVMRP downstream dependent routers:

1. Select Route Table from the Routing > DVMRP group on the web agent window. The DVMRP Route Table dialog box opens (see Figure 9-28).
2. Select the number from the Downstream Dependent Router(s) column for the appropriate source network. The Downstream Dependent Router(s) dialog box opens.

3. Refer to Table 9-26 for an explanation of the DVMRP Downstream Dependent Router(s) dialog box parameters.s

Table 9-26. DVMRP Downstream Dependent Router(s) Dialog Box Parameter

Parameter	Definition
Router Network Address	Displays the router network address of the downstream dependent router.
Found on Interface	Displays the name of the interface on which the downstream router was found.
DVMRP Supported Major/Minor Version	Displays the DVMRP version supported.
Router Received Probe from This Router	Displays whether the router received a probe from this router.
Router Supports Prune Function	Displays whether this router supports prune functionality.
Router Supports Generation ID Function	Displays whether the router supports generation ID function.
Router is SNMP Manageable	Displays whether the router can be managed by SNMP.

Displaying the DVMRP Multicast Forwarding Cache

The DVMRP Multicast Forwarding Cache screen provides detailed information on the multicast forwarding attributes including information on downstream interfaces and upstream sources. DVMRP allows the switch to construct paths from the hosts that are sending to a multicast group to the hosts that are receiving it.

To display the multicast forwarding cache screen:

1. Select Multicast Forwarding Cache from the Routing > DVMRP group on the web agent window. The Multicast Forwarding Cache dialog box opens.
2. To modify the Multicast Forwarding Table:
   - Select the entry and click Delete Entry to delete one or more entries.
   - Click Flush Table to clear the entire table.
   - Click REFRESH to receive the most up-to-date information on the entries in the table.

3. Refer to Table 9-27 for an explanation of the Multicast Forwarding Cache dialog box parameters:

Table 9-27. Multicast Forwarding Cache Dialog Box Parameters

Parameter	Defines the...
Select	Selection of the multicast forwarding cache.
Destination Group Address	Destination group address of the multicast transmission.
Source SubNetwork	Subnet from which the flow is coming.
Source Address Mask	Subnet mask associated with the DVMRP source subnetwork.
Upstream Interface	Local interface which is receiving this flow.
Upstream Neighbor (Router) Address	IP address of the upstream neighbor (router).
Invalid Flows From Upstream	Number of invalid flows received from the upstream neighbor.
Packets Forwarded Through Cache Entry	Number of packets successfully forwarded in the CPU (supervisor module) for this flow.
Upstream Interface is Pruned	Router that is sending prunes to the upstream neighbor. Allows you to open the DVMRP Upstream Prune Information dialog box.
Next Pruned Downstream Interface to Timeout	Next interface that is currently pruned which will be grafted back.
Downstream Interface(s)	Number of downstream interfaces. Allows you to open the DVMRP Downstream Links dialog box.
Upstream Source(s)	Number of upstream interfaces. Allows you to open the Upstream Sources dialog box.

4. Select the number in the Upstream Interface is Pruned field. The Upstream Prune Information dialog box opens.

5. Refer to Table 9-28 for an explanation of the Upstream Prune Information dialog box parameters.

s

Table 9-28. Upstream Prune Information Dialog Box Parameter

Parameter	Displays the...
Destination Group Address	Destination group address of the multicast session.
Source SubNetwork	Subnet on which the DVMRP interface exists.
DVMRP Upstream Interface	Name of the upstream interface.
Interface Type	The interface type. Types include: • **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation. • **IPIP Tunnel** - All multicast traffic (data and protocol messages) on this interface is encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP). • **Non-Encapsulated Tunnel** - All multicast data traffic on this interface is IPIP encapsulated, but the protocol messages are simple unicast.
Interface is Pruned	Status of whether the interface has been pruned.
Prune Expiration Time in sec	Time (in seconds) that the interface times out waiting for the prune message to expire.

6. Select the number in the Downstream Interface(s) field. The DVMRP Downstream Link(s) dialog box opens.

7. Refer to Table 9-29 for an explanation of the DVMRP Downstream Links dialog box parameters.

Table 9-29. DVMRP Downstream Links Dialog Box Parameters

Parameter	Displays the...
Destination Group Address	Destination group address.
Source SubNetwork	Source subnetwork.
DVMRP Downstream Interface	DVMRP Downstream interface.
Interface Type	Interface type. Types include: • **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation. • **IPIP Tunnel** - All multicast traffic (data and protocol messages) on this interface is encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP). • **Non-Encapsulated Tunnel** - All multicast data traffic on this interface is IPIP encapsulated, but the protocol messages are simple unicast.
Interface is Pruned	Status of whether the interface has been pruned.
Prune Expiration in (sec)	Time (in seconds) that the interface times out waiting for the prune message to expire.

8. Select the number in the Upstream Source(s) field. The DVMRP Upstream Source(s) dialog box opens.

9. Refer to Table 9-30 for an explanation of the DVMRP Upstream Source(s) dialog box parameters..

Table 9-30. DVMRP Upstream Source(s) Dialog Box Parameters

Parameter	Displays the...
Destination Group Address	Destination group address for the upstream interface.
Flow Source Address	Host source address for the upstream flow.
Flow Upstream Interface	Name of the flow source interface.
Payload Protocol Type	Protocol type for the payload.
Source Port Number	Source port number.
Destination Port Number	Destination port number.

Configuring Virtual Redundant Router Protocol (VRRP)

You can use VRRP to provide fast automatic fail-over for hosts if the default gateway fails when you have multiple routers to forward traffic configured on your switch. This eliminates the single point of failure inherent in the static default routed environment. A Master VRRP router controls the IP addresses associated with the virtual router and forwards packets sent to these IP addresses. The backup router is always on standby. If the Master router fails, the backup router takes over. Multiple virtual routers can be created per interface. VRRP can be enabled or disabled globally or on an interface basis.

Globally Enabling VRRP

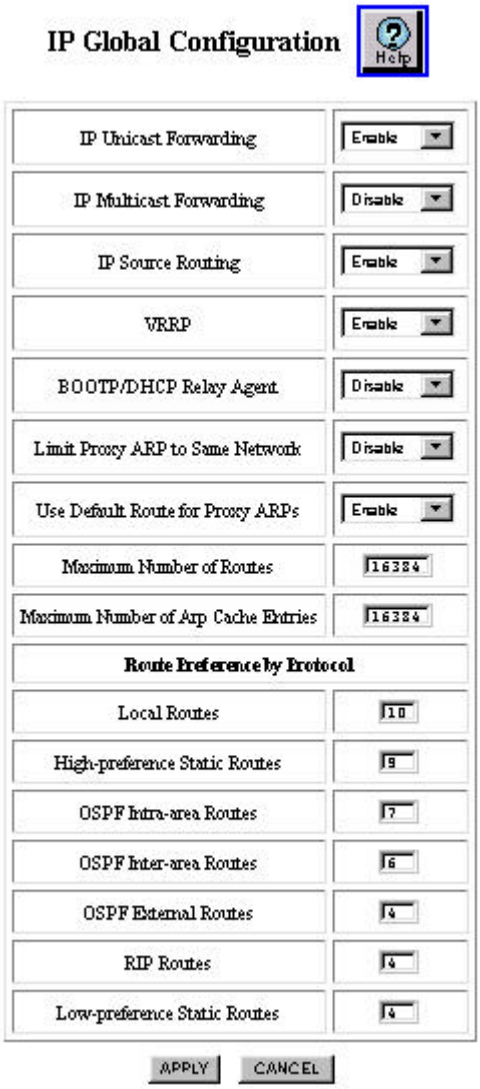
You can globally enable VRRP from either the web agent or the CLI.

Globally Enabling VRRP Using the Web Agent

To globally enable VRRP using the web agent:

1. Select Global Configuration from the Routing > IP > Configuration group on the web agent window. The IP Global Configuration dialog box opens (Figure 9-30).

Figure 9-30. IP Global Configuration Dialog Box



2. Select Enable from the VRRP field pull-down menu.
3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Globally Enabling VRRP Using the CLI

To globally enable VRRP from the CLI, enter the following command in Interface mode:

```
cajun(config-if:ethernet)# ip vrrp
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Enabling VRRP on an Interface

You can enable VRRP on an interface using either the web agent or the CLI.

*** Note:** You must first enable VRRP globally before you can enable VRRP on an interface. Refer to the "Globally Enabling VRRP" section.

Enabling VRRP on an Interfere Using the Web Agent

To enable an VRRP on an interface using the web agent:

1. Select Interfaces from the Routing > IP > Configuration group on the web agent window. The IP Interfaces dialog box opens (Figure 9-31).

   *** Note:** Due to the length of the IP Interfaces dialog box, it is divided into two figures in Figure 9-31.

Figure 9-31. IP Interface Dialog Box

IP Interfaces

Select	State	Interface	Admin. State	VLAN	Network Address	Mask	MAC Format	ARP Timeout
☐	UP	hforew	UP	Default	2.3.4.5	255.255.255.0	Ethernet V2	360
☐	UP	jerry	UP	Default	198.162.99.60	255.255.255.0	Ethernet V2	360
☐	UP	Internal-Network	UP	Internal-Network	10.2.2.1	255.255.255.240	Ethernet V2	360
☐	UP	192.168.99.60	UP	Ethernet-Console	192.168.99.60	255.255.255.0	Ethernet V2	360

APPLY CREATE DELETE CANCEL

IP Routing	RIP	OSPF	Multicast Protocol	Proxy ARP	ICMP Redirect	NetBIOS UDP Rebroadcast	VRRP	BOOTP/DHCP Relay Gateway
Routing/Mgmt	Disable	Enable	DVMRP	Disable	Enable	Disable	Disable	Disable
Routing/Mgmt	Disable	Disable	DVMRP	Disable	Enable	Disable	Disable	Disable
Mgmt Only	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable
Mgmt Only	Disable	Disable	N/A	Disable	Disable	Disable	Disable	Disable

2. Select the interface that you want to enabled.

3. Select Enable from the VRRP field pull-down menu for the interface you selected.

4. Click APPLY to save your changes, or CANCEL to restore previous settings.

Enabling VRRP on an Interface Using the Web Agent

To enable an VRRP on an interface using the CLI, enter the following command in Configure mode:

```
>(configure)# ip vrrp <vr-id> address <ip-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating a VRRP Virtual Router

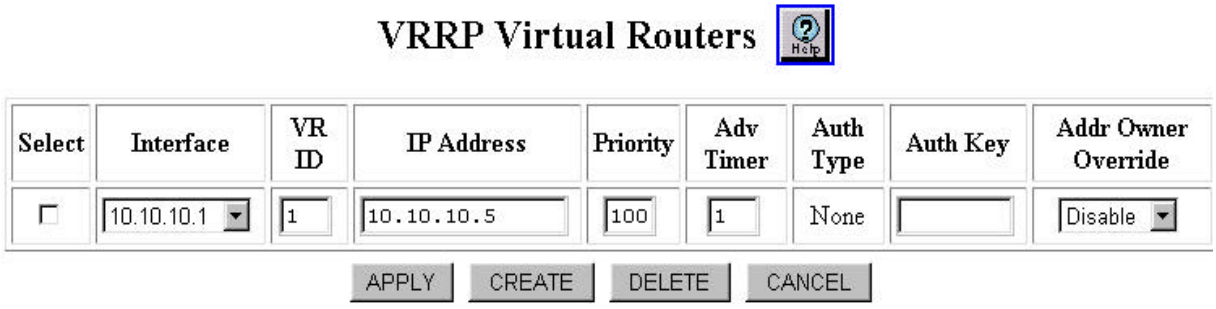
You can create a VRRP router using either the web agent or the CLI.

Creating a VRRP Virtual Router Router Using the Web Agent

To create a VRRP router from the web agent:

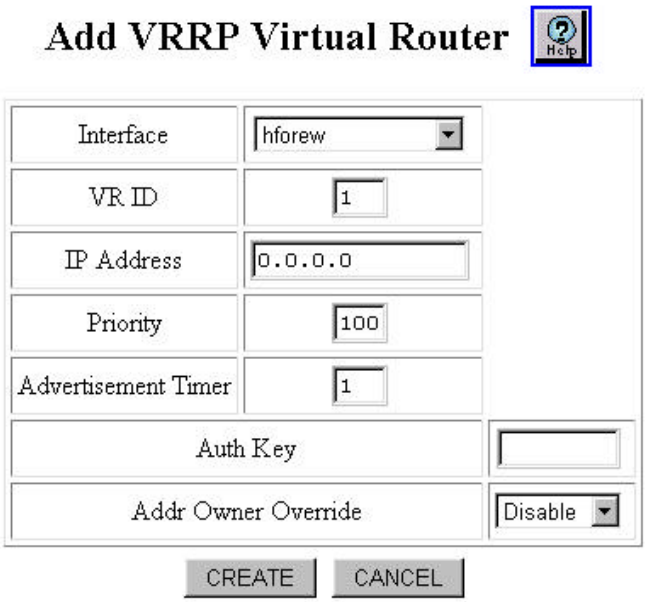
1. Select VRRP from the Routing > IP > Configuration group on the web agent window. The VRRP Virtual Routers dialog box opens (Figure 9-32).

Figure 9-32. VRRP Virtual Routers Dialog Box



2. Select CREATE. The Add VRRP Virtual Router dialog box opens (Figure 9-33).

Figure 9-33. Add VRRP Virtual Router Dialog Box



3. Configure the Add VRRP Virtual Router dialog box parameters for the new VRRP virtual router. Refer to Table 9-31 for an explanation of the Add VRRP Virtual Router dialog box parameters:

Table 9-31. Add VRRP Virtual Router Dialog Box Parameters

Parameter	Defines...
Interface	The name associated with the selected interface.
VR ID	The reporting virtual router's ID. The range is 1-255 (decimal).
IP Address	The virtual router's IP address.
Priority	The sending VRRP router's priority. Higher values equal higher priority. Possible values: • **255** - The value that must be assigned to the Master. • **1** to **254** - Values that must be used for routers backing up a virtual router. • **0** - the current Master is disabled. Allows Backup routers to trigger without waiting for the current Master to timeout.
Advertisement Timer	The time that a Master virtual router advertises itself (sec).

Table 9-31. Add VRRP Virtual Router Dialog Box Parameters continued

Parameter	Defines...
Auth Key	The VRRP authentication key for the interface. The default is AVAYA.
Addr Owner Override	The address owner override.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating a VRRP Virtual Router Router Using the CLI

To create a VRRP router from the CLI, enter the following command in Configure mode:

```
>(config-if:ethernet)# router vrrp
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying VRRP Statistics

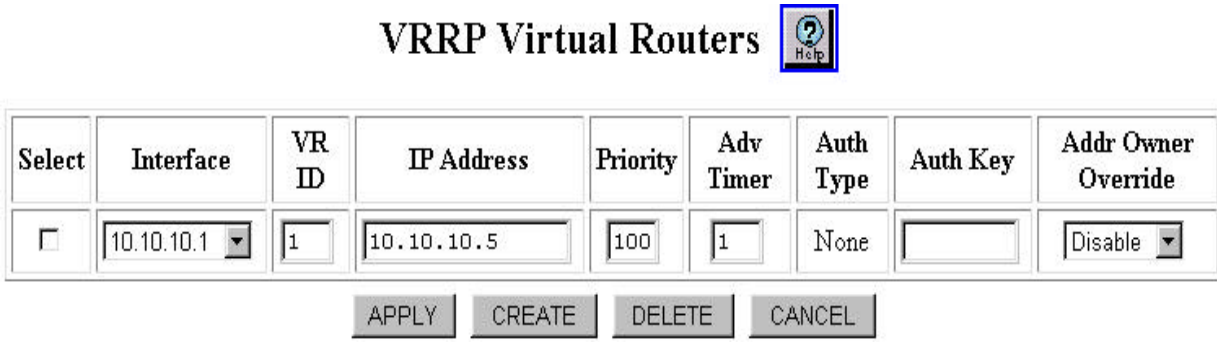
You can display VRRP router statistics using either the web agent or the CLI.

Displaying VRRP Router Statistics using the Web Agent

To view VRRP virtual router statistics using the web agent:

1. Select VRRP Statistics from the Routing > IP > Display group on the web agent window. The VRRP Virtual Router Statistics dialog box opens (Figure 9-34).

Figure 9-34. VRRP Virtual Router Statistics Dialog Box



2. To modify the VRRP statistics:
   - Click CLEAR to reset all the entries.
   - Click REFRESH to receive the most up-to-date information on the entries.

3. Refer to Table 9-32 for an explanation of the VRRP Virtual Router Statistics dialog box parameters:

Table 9-32. VRRP Virtual Router Statistics Dialog Box Parameters

Parameter	Defines the...
Interface	IP interface name corresponding to the selected VRRP virtual router.
VR ID	Reporting virtual router's identification.
IP Address	IP address that corresponds with the selected VRRP virtual router.
State	State of the virtual router. Values include: • **Inactive** - Disables the VRRP virtual router. • **Initialize** - Initializes the VRRP Virtual Router. • **Backup** - Defines the VRRP Virtual Router as a backup router to the master. • **Master** - The VRRP Virtual Router functions as the forwarding router.
Time of State Change	Last state of transition. This value is reported in an HH:MM:SS format.
Times this VR became master	Number of instances that the virtual router became the Master.
Advertisements Received	Number of advertisements received, matching the VRRP Virtual Router configuration.
Advertisements Sent	Number of advertisements sent by the VRRP Virtual Router.
Bad Advertisements Received	Number of advertisements received by the VRRP Virtual Router with invalid parameters.

Displaying VRRP Router Statistics using the CLI

To view VRRP virtual router statistics using the CLI, enter the following command in User mode:

```
cajun> show ip vrrp [cr|<if-name>|<detail>]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring ICMP Router Discovery Protocol (IRDP)

IRDP is an alternative router discovery protocol using ICMP messages on multicast links. ICMP uses router discovery messages, known as router advertisements and router solicitations.

Each router periodically multicasts a router advertisement from each of its multicast interfaces, announcing the IP address of that interface, and other router IP addresses. Hosts discover the addresses of their neighbor routers by listening for the advertisements. When a host attached to a multicast link starts up, it may multicast a router solicitation to ask for immediate advertisements, rather than waiting for the next periodic one to arrive.

If no advertisements arrive, the host re-transmits the solicitation, but does not send additional solicitations. Routers that subsequently start up, or were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

Enabling IRDP on an Interface

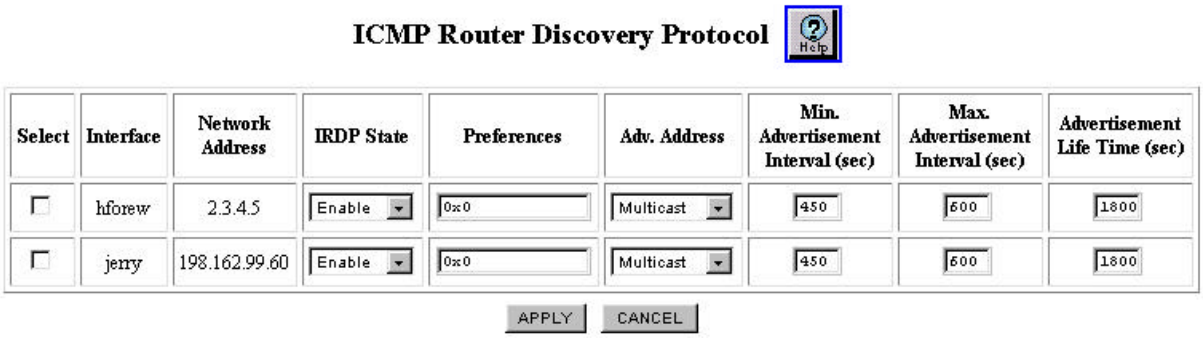
You can enable IRDP on an interface using either the web agent or the CLI.

Enabling IRDP on an Interface Using the Web Agent

To enable IRDP on an interface using the web agent:

1. Select IRDP from the Routing > IP > Configuration group on the web agent window. The ICMP Router Discovery Protocol dialog box opens (Figure 9-35).

Figure 9-35. ICMP Router Discovery Protocol Dialog Box



2. Select the interface on which to enable IRDP in the Select column. A checkmark displays.

3. Refer to Table 9-33 to configure the ICMP Router Discovery Protocol dialog box parameters.

Table 9-33. ICMP Router Discovery Protocol Dialog Box Parameters

Parameter	Allows You to ...
Select	Select the interface to be configured.
Interface	View the IRDP interface name.
Network Address	View the network IP address of the IRDP interface.
IRDP State	Select Disable IRDP on the selected interface. The default value is **Enable**.
Preferences	Enter the preference of the address as a default router address, relative to other router addresses on the same subnet. The minimum value (80000000 hex) is used to indicate that the address should not be used by neighboring hosts as a default router address, even though it may be advertised. The default value is **0**.
Adv. Address	Select an IP destination address used for multicast router advertisements sent from the interface. Options include: • **Multicast** - Used on any link where listening hosts support IP multicast. The default value is 224.0.0.1. • **Broadcast** - Used on any link where listening hosts support IP unicast. The default value is 255.255.255.255.
Min. Advertisement Interval (sec)	Enter the minimum time (in seconds) that is allowed between sending unsolicited multicast router advertisements from the interface. This value must be no less than three seconds and no greater than the Max. Advertisement Interval. The default value is **0.75 times the maximum interval**.

Table 9-33. ICMP Router Discovery Protocol Dialog Box Parameters continued

Parameter	Allows You to ...
Max. Advertisement Interval (sec)	Enter the maximum time (in seconds) allowed between sending multicast router advertisements sent from the interface. This value must be no less than four seconds and no greater than **1800** seconds. The default value is **1800 seconds**.
Advertisement Life Time (sec.)	Enter the time (in seconds) of the life of a router advertisement that is sent from the interface. This value must be no less than the maximum advertisement interval and no greater than **9000** seconds. The default value is **three times the maximum advertisement interva**l.

4. Select Enable from the IRDP State pull-down menu.

5. Select Multicast from the Adv. Address pull-down menu.

6. Delete the default value in the Min. Advertisement Interval (sec.) field and enter the minimum time interval that passes before the host contacts the switch.

7. Delete the default value in the Max. Advertisement Interval (sec.) field and enter the maximum time interval that passes before the host contacts the switch.

8. Delete the default value in the Advertisement Life Time (sec.) field, and enter a duration, in seconds, of the IRDP advertisement.

9. Click APPLY to save your changes, or CANCEL to restore previous settings.

10. Select Global Configuration from the Routing > IP > Configuration group on the web agent window. The IP Global Configuration dialog box opens (see Figure 9-30).

11. Select Enable the IP Multicast Forwarding field pull-down menu.

12. Click APPLY to save your changes, or CANCEL to restore previous settings.

Enabling IRDP on an Interface Using the CLI

To enable IRDP on an interface using the CLI, enter the following command in **Priv** mode:

```
cajun# ip irdp
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring Lightweight Directory Access Protocol (LDAP)

LDAP allows you to access control lists that you can retrieve from a database on an LDAP server and apply them to the Cajun P550/P880/P882 switch.

You can also:

- View LDAP statistics for the switch
- Configure a primary and secondary LDAP server
- Configure a search base for the switch to contact in response to an LDAP request.

Configuring a secondary server ensures that LDAP requests can be fulfilled if a primary server fails. The LDAP client sends a search for access control lists to the primary server if the client finds the primary server. The primary server retrieves the access lists from the LDAP database and returns them to the switch's LDAP client. If the client does not find the primary server and if the primary server does not respond after five retries, the client tries to connect to the secondary server. If the secondary server fails after five retries, the client times out. The LDAP client applies the access lists to manage the way traffic is forwarded.

Configuring LDAP Settings

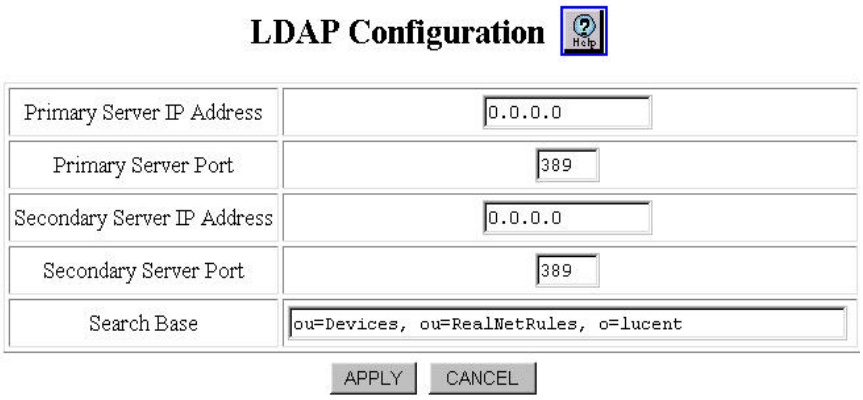
You can configure LDAP settings from either the web agent or the CLI.

Configuring LDAP Settings from the Web Agent

To configure LDAP settings from the web agent:

1. Select LDAP Configuration from the Routing > IP > Configuration group on the web agent. The LDAP Configuration dialog box opens (Figure 9-36).

Figure 9-36. LDAP Configuration Dialog Box



2. Refer to Table 9-34 to configure the LDAP Configuration dialog box parameters.

Table 9-34. LDAP Configuration Dialog Box Parameters

Parameter	Allows You To ...
Primary Server IP Address	Enter the IP address of your primary LDAP server for the access control list domain. This address is used first when connecting to and downloading access lists from an LDAP server. The default value of 0.0.0.0 indicates to the client that there is no primary LDAP server.
Primary Server Port	Enter the **port number** of the primary LDAP server for the access control list domain. The port number is used in conjunction with the primary server IP address. There are no special overload values. The default port is 389.

Table 9-34. LDAP Configuration Dialog Box Parameters continued

Parameter	Allows You To ...
Secondary Server IP Address	Enter the backup LDAP server IP address for the access control list domain. This address is used as a backup when connecting to and downloading access lists from an LDAP server. If the LDAP client is unsuccessful in connecting to or downloading access lists from the primary server, the secondary server IP address is used. If the primary server IP address has a value of 0.0.0.0, the secondary server IP address is used. The default value is 0.0.0.0. **Note:** Setting the IP address of the secondary server to 0.0.0.0 indicates to the LDAP client that there is no secondary server.
Secondary Server Port	Enter the backup LDAP server port number for the access control list domain. The port number is used in conjunction with the secondary server IP address. There are no special overload values. The default port number is 389.
Search Base	Enter the search criteria that will be sent to the LDAP server. The default value is "ou=Devices, ou=CajunRules, o=Avaya".

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring LDAP Settings from the CLI

To configure LDAP settings on a primary server from the CLI, enter the following command from configuration mode:

```
cajun (configure)# ldap server primary <ip-addr>
[<port-num>]
```

To configure LDAP settings on a secondary server from the CLI, enter the following command from configuration mode:

```
cajun (configure)# ldap server secondary <ip-addr>
[<port-num>]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing LDAP Statistics

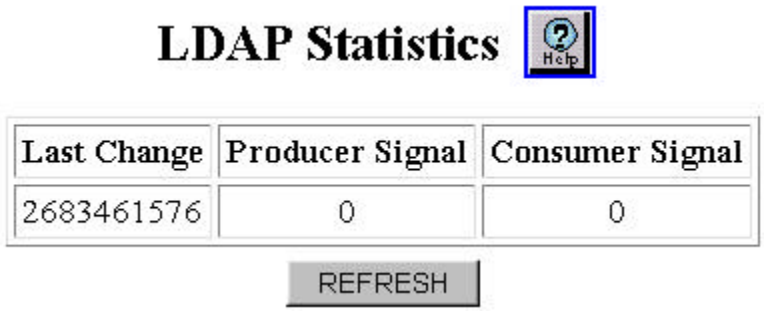
You can view LDAP statistics from either the web agent or the CLI.

Viewing LDAP Statistics Using the Web Agent

To view LDAP statistics using the web agent:

1. Select LDAP Statistics from the Routing > IP > Display group on the web agent window. The LDAP Statistics dialog box opens (Figure 9-37).

Figure 9-37. LDAP Statistics Dialog Box



2. Click Refresh to dynamically update LDAP Statistics parameters.

3. Refer to Table 9-35 for an explanation of the LDAP Statistics dialog box parameters:

Table 9-35. LDAP Statistics Dialog Box Parameters

Parameter	Definition
Last Change	Displays the **sysUpTime** since this device was last modified. You can detect a change in the Policy Capabilities by polling a single object using this information. For detailed information about **SysUpTime** and P**olicy Capabilities**, refer to AvayaDevicePolicyCapabilityLastChange in the Avaya MIB.
Producer Signal	The sequence number that, when modified, triggers the LDAP client to download the latest policy from the LDAP server. Typically, RealNet Rules will set this value whenever there is a new policy to download. If this value is a non-zero value, the LDAP client will compare it to the producer signal on the LDAP server. No comparison is made if the value is zero.
Consumer Signal	Indicates the success of the LDAP client when downloading a policy. If the consumer signal matches the producer signal, downloading LDAP to a policy was successful. If the consumer signal is -1, then either the LDAP client had a problem processing the access lists or the consumer signal set on the LDAP client did not match the signal configured on the LDAP server. If the consumer signal is not -1 and does not match the producer signal, then the LDAP client was unable to connect to the LDAP server(s).

Viewing LDAP Statistics Using the CLI

To view LDAP statistics using the CLI, enter the following command:

```
show ldap
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

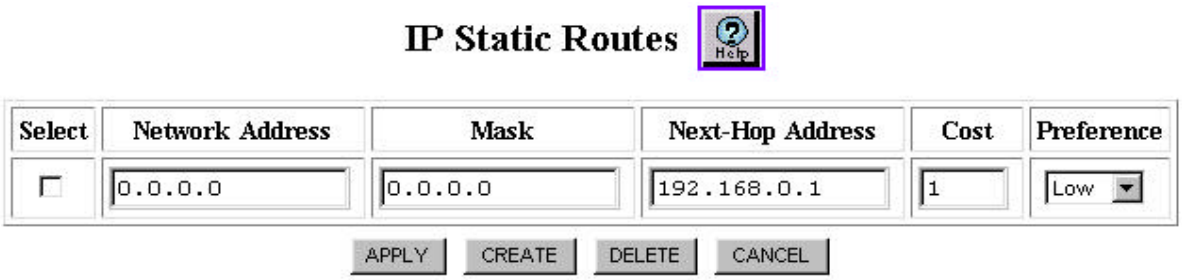
Configuring a Static Route for the PPP Console

To configure a PPP Console static route:

1. Configure your console serial port as a PPP Console. Refer to the “Connecting a Modem” section in Chapter 2, *Initialize and Setup of the P550/P880/P882 Switch*.

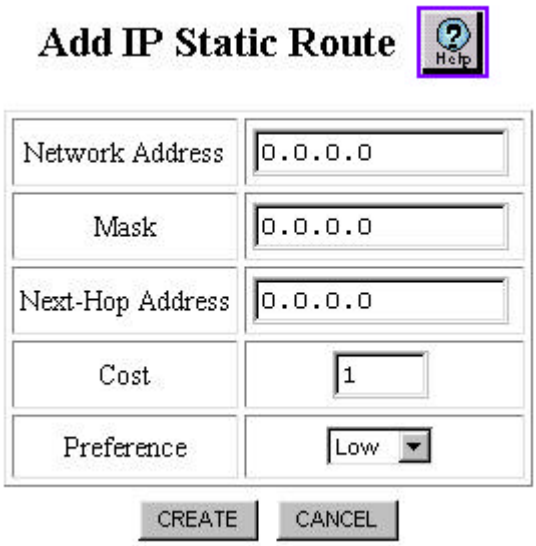
2. Select Static Routes from the Routing > IP > Configuration folders on the web agent window. The IP Static Routes dialog box opens (Figure 9-38).

Figure 9-38. IP Static Routes Dialog Box



3. Select CREATE. The Add IP Static Routes dialog box opens (Figure 9-39).

Figure 9-39. Add IP Static Routes Dialog Box



4. Enter the IP address that is to be associated with the PPP console port in the Network Address field.

5. Enter the network mask IP address in the Mask field.

6. Enter the IP address of the gateway associated with this static route in the Next-Hop Address field.

7. Click CREATE to save your changes, or CANCEL to restore previous settings. The IP Static Routes window re-opens.

8. Click APPLY to save your changes, or CANCEL to clear your selection.

Configuring the IP Interface for the PPP Console

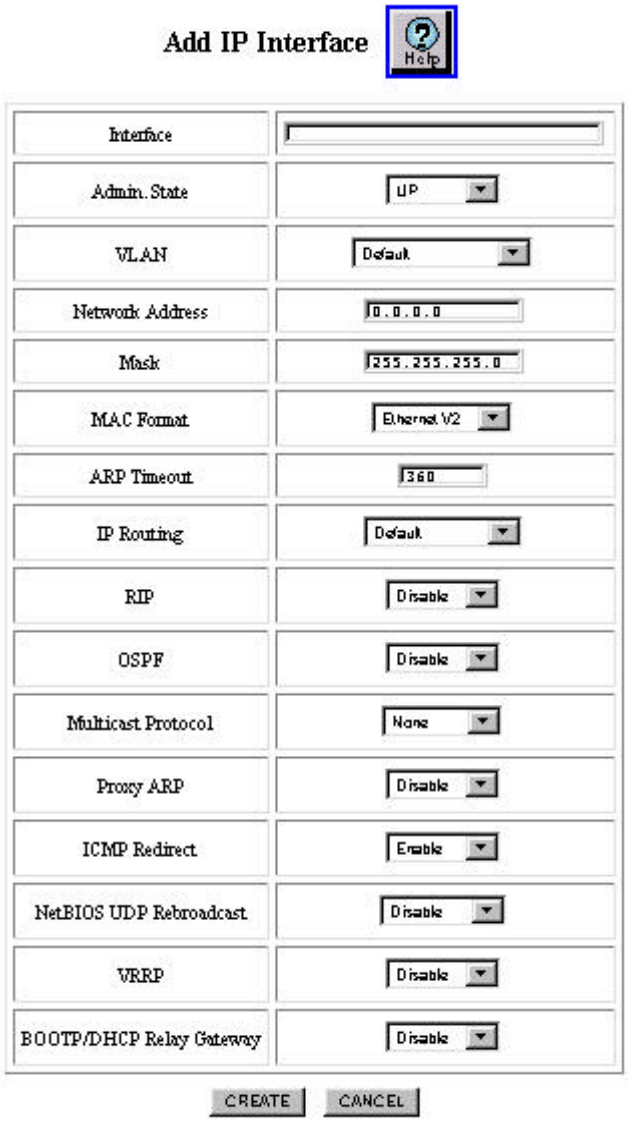
You can configure an IP interface for the PPP console from either the web agent or the CLI.

Configuring the IP Interface for the PPP Console Using the Web Agent

To configure the PPP console with an IP address and mask using the web agent:

1. Configure your console serial port as a PPP Console. See "Connecting a Modem", in Chapter 2, Initialize and Setup of the P550/P880/P882 Switch.
2. Connect your modem cable to the switch's serial port.
3. Select Interfaces from the Routing > IP > Configuration group on the web agent window. The IP Interfaces dialog box opens (Figure 9-31).
4. Select CREATE. The Add IP Interface dialog box opens (Figure 9-40).

Figure 9-40. Add IP Interface Dialog Box



5. Select Serial-Console from the VLAN field pull-down menu. This indicates the interface for the PPP console.

6. Enter the IP address in the Network Address field that is to be associated with the PPP console port. If you do not enter a name for this interface, the IP address is used.

7. Enter the network mask IP address in the Mask field (for example, 255.255.255.0).

8. Click CREATE to save your changes, or CANCEL to restore previous settings. The IP Interfaces window re-displays.

9. Click APPLY to save your changes, or CANCEL to clear your selection.

Configuring the IP Interface for the PPP Console Using the CLI

To configure the PPP console after you have made all the applicable cable connections with an IP address using the CLI, enter the following command in Interface mode:

```
cajun (config if <interface-name>)# ip vlan
{<vlan-id>|name <vlan-name>| Ethernet-
Console|Serial-Console}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

10 Configuring the Routing Information Protocol (RIP)

Overview

*** Note:** You must globally enable RIP before it can be configured. To globally enable RIP, refer to “Creating an IP Interface”, and “Configuring Virtual Redundant Router Protocol (VRRP)”, in Chapter 9, "Configuring IP Routing".

The information and procedures provided in this chapter pertain to layer 3 module configuration only:

This section describes:

- Configuring RIP on the Switch
- Modifying RIP Interfaces
- Creating Trusted RIP Neighbors
- Viewing RIP Statistics

Configuring RIP on the Switch

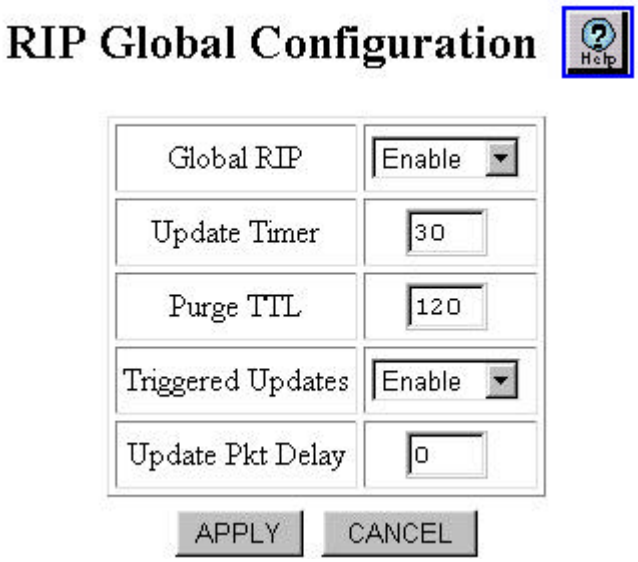
You can configure the RIP from either the web agent or the CLI.

Configuring RIP on the Switch Using the Web Agent

To configure the RIP globally on your switch using the web agent:

1. Select Global Configuration from the Routing > IP > RIP group on the Web Agent window. The RIP Global Configuration dialog box opens (Figure 10-1).

Figure 10-1. RIP Global Configuration Dialog Box



2. Refer to Table 10-1 to configure the RIP Global Configuration dialog box parameters:

Table 10-1. RIP Global Configuration Dialog Box Parameters

Parameter	Allows you to...
Global RIP	Enable or disable the RIP protocol. The default is Enable.
Update Timer	Enter the value (in seconds) that represents the time between RIP updates on all interfaces. The default value is 30 seconds.
Purge TTL	Enter the global Time To Live (TTL) in seconds that the RIP update persists. The default value is 120 seconds.
Triggered Updates	**Disable** route updates that were triggered by a topology change in the network to be added to the routing table. The default is **Enable**.
Update Pkt Delay	Enter the value (in seconds) that represents the time delay between successive RIP update packets to the neighbor, when the update requires multiple packets. The default value is 0 seconds (no delay).

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring RIP on the Switch Using the CLI

To configure the RIP globally on your switch using the CLI, enter the following command in Configure mode:

```
cajun (configure)# router rip
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying RIP Interfaces

You can modify RIP interfaces from either the web agent or the CLI.

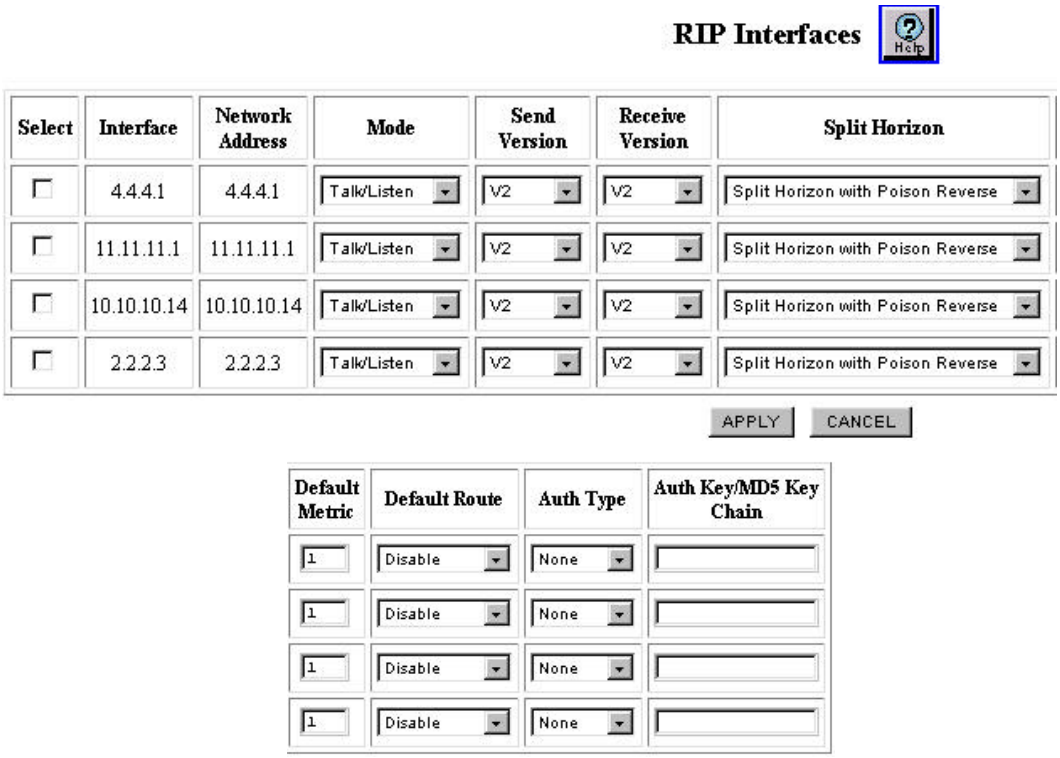
Modifying RIP Interfaces Using the Web Agent

To modify RIP interfaces using the CLI from the web agent:

1. Select Interfaces from the Routing > IP > RIP group on the Web Agent window. The RIP Interfaces dialog box opens (Figure 10-2).

***Note:** Due to its length, the RIP interface dialog box is divided into two parts in Figure 10-2.

Figure 10-2. RIP Interfaces Dialog Box



2. Refer to Table 10-2 to modify the RIP interfaces dialog box parameters:

Table 10-2. RIP Interface Dialog Box Parameters

Parameter	Allows you to...
Select	Select the RIP interface to be modified.
Interface	Displays an interface from a list of interfaces that you previously configured.
Network Address	Displays an IP address to be associated with the displayed interface.
Mode	Specify the RIP State. Different states include: • **talk only** (send RIP information to the network) • **listen only** (receive RIP information from the network) • **talk/listen** (both send and receive RIP information from the network)
Send Version	Specify the version of RIP you want to use to send packets across your interface. Selections include: • V1 • V2 • V1/V2
Receive Version	Specify the version of RIP you want to use to receive packets. Selections include: • V1 • V2 • **V1/V2**
Split Horizon	Specify that IP routes learned from an immediate neighbor are not advertised back to the neighbor from which the routes were learned. • **Split Horizon** - Routes are not advertised. • **Split Horizon with Poison Reverse** - Routes are advertised with an infinite metric (16).
Default Metric	Specify the default RIP route metric value.

Table 10-2. RIP Interface Dialog Box Parameters continued

Parameter	Allows you to...
Default Route	Specify the mode for the default route. Different states include: • **Disable** - Disables the default route. • **Talk Only** - Send RIP information to the network. • **Listen Only** - Receive RIP information from the network. • **Talk/Listen** - Both send and receive RIP information from the network.
Auth Type	Specify the type of authentication available for use on a given RIP interface. Authentication types include: • **None** - No authentication available. • **Simple** - Uses a clear-text password for validation. • **MD5** - Uses a stronger encryption technique for passwords.
Auth Key	Enter the authorization key value.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Modifying RIP Interfaces Using the CLI

To modify RIP interfaces using the CLI enter the following command from Configure mode:

```
> (configure)# route rip <cr>
> (configure router rip)# interface
   <interface name|interface range>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating Trusted RIP Neighbors

Trusted RIP neighbors enable you to enhance a Cajun switch's security by enabling one or more neighbors to relay RIP information.

*** Note:** Adding one or more trusted RIP neighbors ensures that your router accepts only information from these neighbors. Consequently, all other information is filtered. Do not create trusted RIP neighbor(s) if you do not wish to filter RIP information from the network.

You can create a trusted neighbor using either the web agent or the CLI.

Creating Trusted RIP Neighbors Using the Web Agent

To create a trusted RIP neighbor using the web agent:

1. Select Trusted Neighbors from the Routing > IP > RIP group on the web agent window. The RIP Trusted Neighbors dialog box opens (Figure 10-3).

Figure 10-3. RIP Trusted Neighbors Dialog Box

2. Click CREATE. The Add Trusted RIP Neighbor dialog box opens (Figure 10-4).

Figure 10-4. Add Trusted RIP Neighbors Dialog Box

3. Enter the network address for the node that acts as the trusted RIP neighbor in Network Address field.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating Trusted RIP Neighbors Using the CLI

To create a trusted RIP neighbor using the CLI enter the following command from **Configure** mode:

```
> (configure)# route rip <cr>
> (configure router rip)# neighbor <ip-addr>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Viewing RIP Statistics

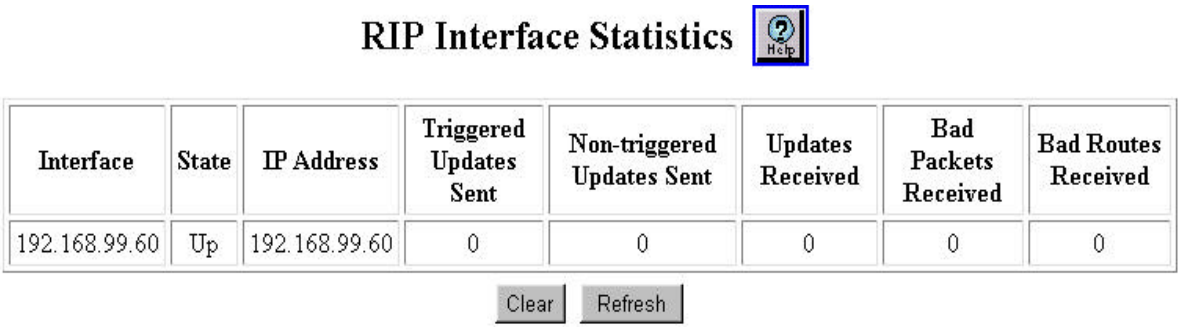
You can view RIP statistics using either the web agent or the CLI.

Viewing RIP Statistics Using the Web Agent

To view RIP statistics using the web agent:

1. Select Interface Statistics from the Routing> IP > RIP group on the web agent window. The RIP Interface Statistics dialog box opens (Figure 10-5).

Figure 10-5. RIP Interface Statistics Dialog Box



2. To modify your RIP statistics:
   - Click CLEAR *to reset all the entries*.
   - Click REFRESH to receive the most up-to-date information on the entries.
3. Use Table 10-3 to interpret the RIP statistics:

Table 10-3. RIP Statistical Parameters

Parameter	Defines the...
Interface	Interface associated with the IP address specified.
State	Current status of the RIP route. UP indicates that the interface is up and RIP can transmit and receive updates.
IP Address	IP address associated with the interface.
Triggered Updates Sent	Number of RIP triggered updates sent.
Non-Triggered Updates Sent	Number of RIP non-triggered updates sent.
Updates Received	Number of RIP updates received based on route changes in the IP routing table.
Bad Packets Received	Number of bad packets received on this interface.
Bad Routes Received	Number of bad routes received on this interface.

Viewing RIP Statistics Using the CLI

To view RIP statistics using the CLI, enter the following command from Configure mode:

```
> (configure)# show ip rip statistics
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

11 Configuring the OSPF Routing Protocol

Overview

The following information and procedures provided in this chapter pertain to layer 3 module configuration only:

- Configuring Open Shortest Path First (OSPF)
- Monitoring Switch Performance Using OSPF Statistics

Configuring Open Shortest Path First (OSPF)

This section provides the following information about OSPF:

- Configuring the OSPF Global Configuration
- Creating OSPF Areas
- Deleting OSPF Areas
- Modifying OSPF Areas
- Deleting OSPF Areas
- Creating OSPF Virtual Links
- Deleting OSPF Virtual Links
- Modifying OSPF Virtual Links
- Creating OSPF Summaries
- Deleting OSPF Summaries
- Modifying OSPF Summaries

Configuring the OSPF Global Configuration

The OSPF global configuration allows you to globally configure OSPF on your switch. It also allows you to specify your router ID and whether or not you want the switch to be the Autonomous System (AS) border router.

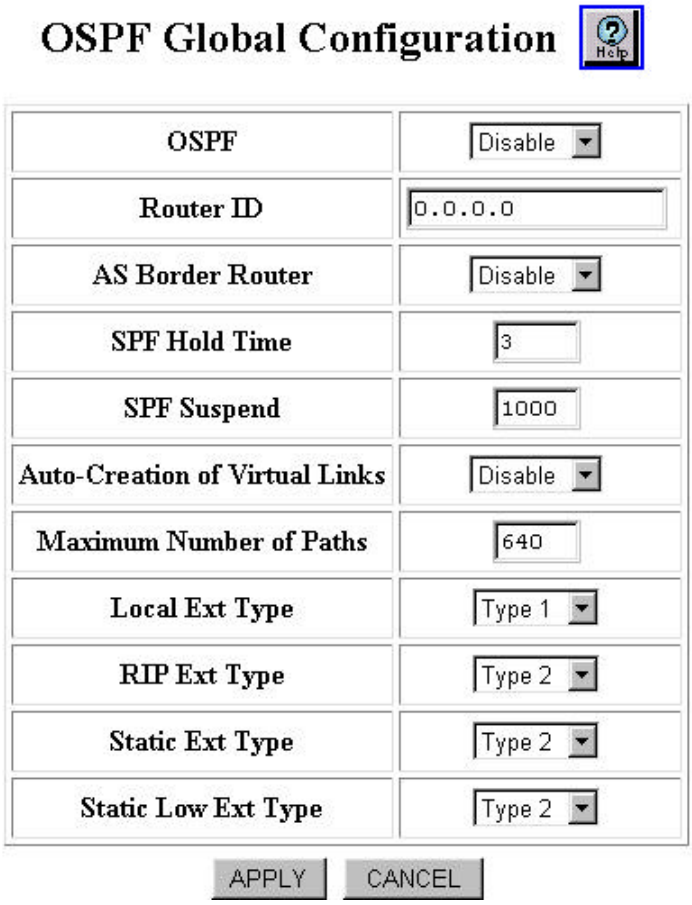
You can globally configure OSPF using either the web agent or the CLI.

Configuring OSPF Globally Using the Web Agent

To globally configure OSPF using the web agent:

1. Select Global Configuration from the System > IP > OSPF group on the web agent window. The OSPF Global Configuration dialog box opens (Figure 11-1).

Figure 11-1. OSPF Global Configuration Dialog Box



2. Refer to Table 11-1 to configure the OSPF Global Configuration dialog box parameters:

Table 11-1. OSPF Global Configuration Dialog Box Parameters

Parameter	Allows you to...
OSPF	Select to enable or disable OSPF globally on your switch.
Router ID	Specify the Router ID on the switch. The router ID is a 32-bit number assigned to each router running OSPF. This number uniquely identifies the router within an Autonomous System. If 0.0.0.0 is used, the router uses the IP address of an interface.
AS Border Router	Enable or disable the switch to be an Autonomous System Border Router (ASBR).
SPF Hold Time	Specify the minimum number of seconds between SPF runs.
SPF Suspend	Specify the number of nodes to process SPF runs before suspending.
Auto-Creation of Virtual Links	Enable or disable the function of automating the creation of virtual circuits based on network topology.
Maximum Number of Paths	Configure the maximum number of paths used when running SPF.
Local Ext Type	Specify whether imported local routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.
RIP Ext Type	Specify whether imported RIP routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.
Static Ext Type	Specify whether imported high preference routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.
Static Low Ext Type	Specify whether imported low preference routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.

3. Click APPLY to save changes, or CANCEL to restore previous settings.

Configuring OSPF Globally Using the CLI

To globally configure OSPF using the CLI, enter the following command in Configure mode:

```
Cajun> (configure)# router ospf
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating OSPF Areas

You can create OSPF areas using either the web agent or the CLI.

Creating OSPF Areas Using the Web Agent

To create OSPF areas using the web agent:

1. Select Areas from the Routing > IP > OSPF group on the web agent window. The OSPF Areas dialog box opens (Figure 11-2).

   Note: The Area ID 0.0.0.0 is a backbone area and always exists in an OSPF configuration.

Figure 11-2. OSPF Areas Dialog Box

2. Click CREATE. The Add OSPF Area dialog box opens (Figure 11-3).

Figure 11-3. ADD OSPF Area Dialog Box

3. Refer to Table 11-2 to configure the Add OSPF Area dialog box parameters:

Table 11-2. Add OSPF Area Dialog Box Parameters

Parameter	Allows you to...
Area ID	Specify the Area ID (32-bit character) for the new area. This must be a unique ID within AS. **Note:** Do not use 0.0.0.0 as an area ID.
Area Type	Select the type of area. Types include: • **Non-Stub** - Non-edge device/router. • **Stub** - An edge device/router that does not leak external advertisements. • **Not-so-stubby** - This is still a stub area, however, this device/router can leak some external advertisements.
Translate 7 into 5	Select to enable or disable the translation of the NSSA ASE Type 7 into an AS External LSA Type 5.
Stub Metric	Specify the stub area default summary cost metric. (Default is 1).
Type 3 ASE Filter	Select to enable or disable the Type 3 summary LSA filter for Stub and NSSA only.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating OSPF Areas Using the CLI

To create OSPF areas using the CLI, enter the following command in **Configure** mode:

```
> (configure router ospf)# area <area-id> <option>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting OSPF Areas

You can delete an OSPF area using either the web agent or the CLI.

Deleting an OSPF Area Using the Web Agent

To delete an OSPF area using the web agent:

1. Select Areas from the Routing > IP > OSPF group on the web agent window. The OSPF Areas dialog box opens (Figure 11-2).
2. Select the OSPF Area to be removed from the Select field.
3. Click DELETE. The OSPF area you selected is deleted.

Deleting an OSPF Area Using the CLI

To delete an OSPF area using the CLI, enter the following command in Configure mode:

```
> (configure)# router ospf [no] area <area-id>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying OSPF Areas

You can modify the parameters of an OSPF area using either the web agent or the CLI.

Modifying an OSPF Area Using the Web Agent

To modify an OSPF area using the web agent:

1. Select Areas from the Routing > IP > OSPF group on the web agent window. The OSPF Areas dialog box opens (Figure 11-2).
2. Select an OSPF Area to be modified from the Select field.
3. Refer to Table 11-2 and modify the OSPF Area dialog box parameters.
4. Click Apply to save your changes, or Cancel to ignore your changes.

Modifying an OSPF Area Using the CLI

To modify an OSPF area using the CLI, enter the following command in **Configure** mode:

```
>(configure router ospf)# area <area-id> <option>
```

Refer to the *Avaya™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying OSPF Interfaces

You can modify the parameters on an OSPF interface using either the web agent or the CLI.

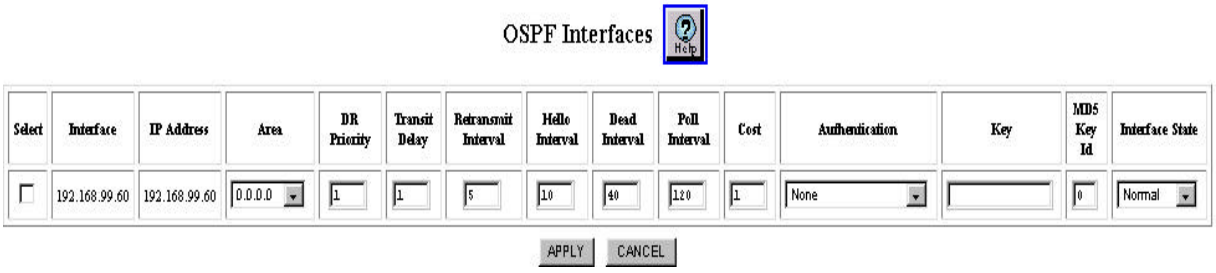
Modifying OSPF Interfaces Using the Web Agent

To modify an OSPF interface using the web agent:

1. Select Interfaces from the Routing > IP > OSPF group in the web agent window. The OSPF Interfaces dialog box opens (Figure 11-4).

   Note: You must first enable OSPF before you can modify OSPF interfaces. Refer to *Configuring a Static Route for the PPP Console* in Chapter 9 for information on how to enable OSPF on IP interfaces.

Figure 11-4. OSPF Interfaces Dialog Box



2. Modify the OSPF Interfaces dialog box parameters. Refer to Table 11-3 for an explanation of these parameters:

Table 11-3. OSPF Interface Dialog Box Parameters

Parameter	Definition
Select	Select the OSPF interface to be modified.
Interface	Displays IP interface (VLAN) that has OSPF enabled. **Note:** This is a read-only field.
IP Address	Displays IP address associated with the OSPF interface. **Note:** This is a read-only field.
Area	Enter the area ID configured for this interface.
DR Priority	Enter the decimal value for this interface for DR priority functionality.
Transit Delay	Enter the estimated time (seconds) it takes to transmit a link state update packet over this interface.

Table 11-3. OSPF Interface Dialog Box Parameters continued

Parameter	Definition
Retransmit Interval	Enter the time (seconds) between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.
Hello Interval	Enter the time (seconds) between the Hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network.
Dead Interval	Enter the time (seconds) that a router's Hello packets have not been seen before it's neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.
Poll Interval	Enter the larger time interval (seconds) between the Hello packets sent to an inactive non-broadcast multiaccess neighbor.
Cost	Enter the cost metric associated with this interface.
Authentication	Select the type of authentication available for use on a given OSPF interface. Authentication types are: • None • Simple Password • MD5 Authentication
Key	Enter the area's authorization key value.
MD5 Key ID	Enter the MD5 authentication key ID as a decimal value.
Interface State	Select the interface state. The available sites are: • Normal • Passive

3. Click Apply to save the changes or Cancel to ignore the changes.

Modifying OSPF Interfaces Using the CLI

To modify an OSPF interface using the CLI, enter the following command from Configure Interface mode:

```
>(configure interface) <interface name> ip ospf <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating OSPF Virtual Links

You can create OSPF Virtual links using either the web agent or the CLI.

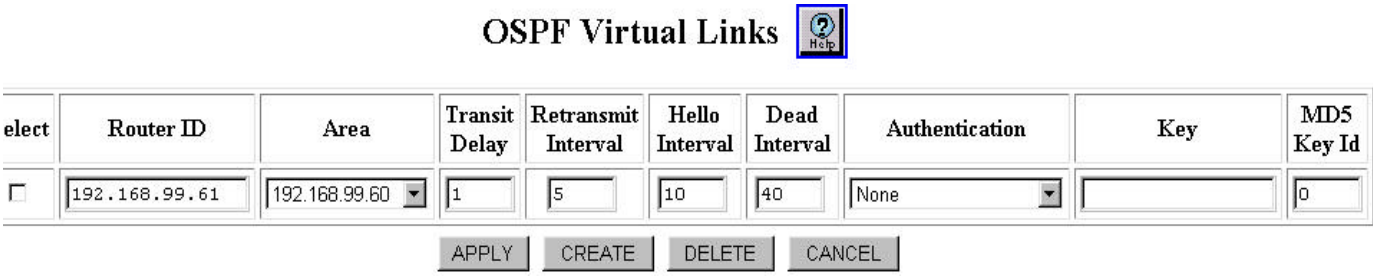
Creating OSPF Virtual Links Using the Web Agent

To create a OSPF virtual link using the web agent:

1. Select Virtual Links from the Routing > IP > OSPF group on the web agent window. The OSPF Virtual Links dialog box opens (Figure 11-5).

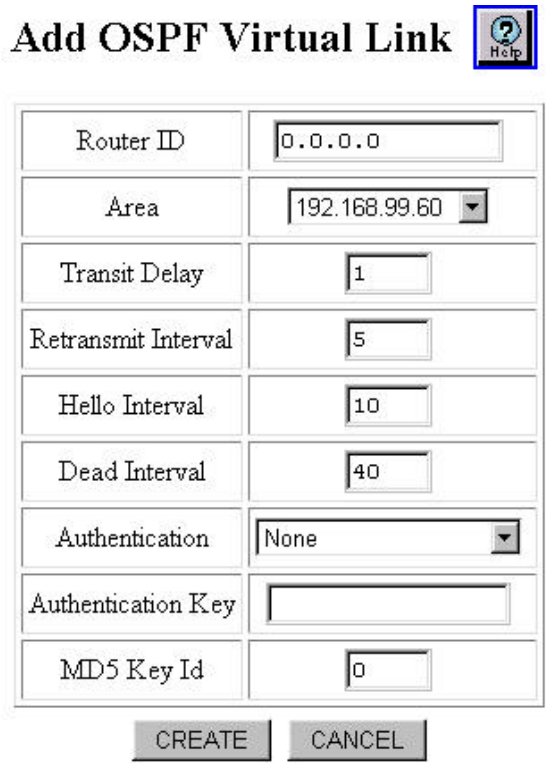
   Note: The OSPF dialog box displays only if OSPF virtual links were previously configured.

Figure 11-5. OSPF Virtual Links Dialog Box



2. Select CREATE. The Add OSPF Virtual Link dialog box opens (Figure 11-6).

Figure 11-6. Add OSPF Virtual Link Dialog Box



3. Enter the new OSPF Link information. Refer to Table 11-4 for an explanation of the Add OSPF Virtual Link dialog box parameters:

Table 11-4. Add OSPF Virtual Link Dialog Box Parameters

Parameter	Defines the...
Router ID	Router ID for the far end of the virtual link.
Area	Area ID through which the virtual link travels.
Transit Delay	Estimated number of seconds it takes to transmit a link state update packet over this virtual link.
Retransmit Interval	Number of seconds between link-state advertisement retransmissions for adjacencies belonging to this virtual link. This value is also used when retransmitting database description and link-state request packets.

Table 11-4. Add OSPF Virtual Link Dialog Box Parameters continued

Parameter	Defines the...
Hello Interval	Time in seconds between the Hello packets that the router sends on the virtual link. This value must be the same for all routers attached to a common network.
Dead Interval	Time in seconds that a router's Hello packets have not been seen before it's neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.
Authentication	Type of authentication available for use on a given OSPF interface. Authentication types include: • None • Simple Password • MD5 Authentication
Authentication Key	Area's authentication key.
MD5 Key ID	MD5 authentication key ID as a decimal value.

4. Click **CREATE** to create the virtual link, or **CANCEL** if you do not want to create the OSPF virtual link.

Creating OSPF Virtual Links Using the CLI

To create a OSPF virtual link using the CLI, enter the following command from Configure mode:

```
>(configure router: ospf) area <area-id> virtual-link
<router-id>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting OSPF Virtual Links

You can delete OSPF Virtual links using either the web agent or the CLI.

Deleting OSPF Virtual Links Using the Web Agent

To delete an OSPF virtual link using the web agent:

1. Select Virtual Links from the Routing > IP > OSPF group on the Web Agent window. The OSPF Virtual Links dialog box opens (Figure 11-5).
2. Select the virtual link that you want to remove.
3. Click DELETE. The virtual link is removed.

Deleting OSPF Virtual Links Using the CLI

To delete an OSPF virtual link using the CLI, enter the following command from Configure mode:

```
Cajun(configure router: ospf)# [no] area <area-id>
virtual-link <router-id>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying OSPF Virtual Links

You can modify OSPF virtual links using either the web agent or the CLI.

Modifying OSPF Virtual Links Using the Web Agent

To modify an OSPF virtual link using the web agent:

1. Select Virtual Links from the Routing > IP > OSPF group on the Web Agent window. The OSPF Virtual Links dialog box opens (Figure 11-5).
2. Select the virtual link that you want to modify.
3. Refer to Table 11-4 to modify the OSPF Virtual Links dialog box parameters.
4. Click APPLY to save your changes, or CANCEL to restore previous settings.

Modifying OSPF Virtual Links Using the CLI

To modify an OSPF virtual link using the CLI, enter the following command and make your desired changes from Configure mode:

```
cajun(configure router: ospf)# area <area-id>
virtual-link <router-id> [hello-interval
<seconds>] [retransmit-interval <seconds>] [dead-
interval <seconds>] [{authentication-key <key> |
message-digest-key <key-id> md5 <key>}]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating OSPF Summaries

The primary purpose of the OSPF summary is route aggregation. Route aggregation is a group range of IP addresses that are linked to a single address.

You can create a new OSPF summary from either the web agent or the CLI.

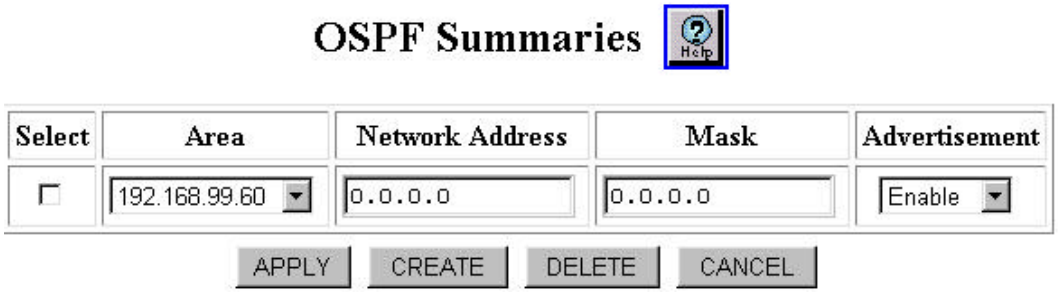
Creating OSPF Summaries Using the Web Agent

To create a new OSPF summary using the web agent:

1. Select Summaries from the Routing > IP > OSPF group on the web agent window,. The OSPF Summaries dialog box opens (Figure 11-7).

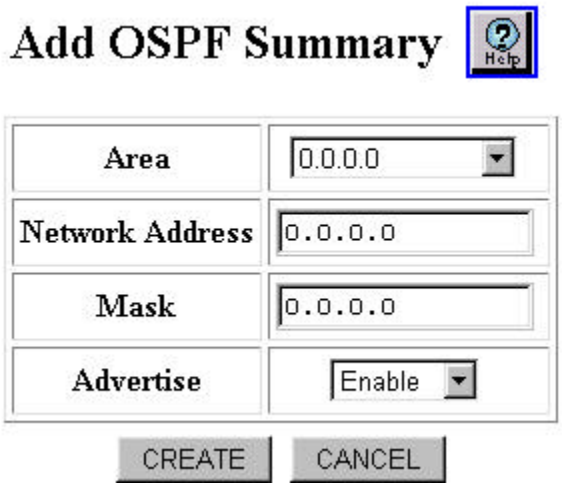
   Note: This dialog box will display OSPF summaries only if you have previously configured one or more summaries.

Figure 11-7. OSPF Summaries Dialog Box



2. Select CREATE. The Add OSPF Summary dialog box opens (Figure 11-8).

Figure 11-8. Add OSPF Summary Dialog Box



3. Refer to Table 11-5 to configure the Add OSPF Summary dialog box parameters:

Table 11-5. Add OSPF Summary Dialog Box Parameters

Parameter	Definition
Area	Select the area ID of the area from which the routes are aggregated (summary IP address).
Network Address	Enter the IP address of the network to be advertised.
Mask	Enter the subnet mask of the network to be advertised.
Advertise	Select the ability to suppress (disable) or enable advertisements of this summary. When suppressing, advertisements of IP routes in this range are also suppressed.

4. Click CREATE to save the new OSPF summary, or CANCEL to ignore the new summary.

Creating OSPF Summaries Using the CLI

To create a new OSPF summary using the CLI, enter the following command from Configure mode:

```
cajun(configure router: ospf)# area <area id>
range (ospf summary network) <ospf-summ>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting OSPF Summaries

You can delete OSPF summaries from either the web agent or the CLI.

Deleting OSPF Summaries Using the Web Agent

To delete an OSPF summary using the web agent:

1. Select Summaries from the Routing > IP > OSPF group on the web agent window. The OSPF Summaries dialog box opens (Figure 11-7).
2. Select the OSPF summary that you want to remove.
3. Click DELETE. The OSPF summary you selected is removed.

Deleting OSPF Summaries Using the CLI

To delete an OSPF summary using the CLI, enter the following command from Configure mode:

```
cajun(configure router: ospf)# [no] area
<area-id> range <ip-address> <mask>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying OSPF Summaries

You can modify an OSPF summary using wither the web agent or the CLI.

Modifying OSPF Summaries Using the Web Agent

To modify an OSPF summary using the web agent:

1. Select Summaries from the Routing > IP > OSPF group on the web agent window. The OSPF Summaries dialog box opens (Figure 11-7).
2. Select the OSPF summary to be modified.
3. Refer to Table 11-5 to configure the OSPF Summaries dialog box parameters.
4. Click APPLY to save your changes, or CANCEL to restore previous settings.

Modifying OSPF Summaries Using the CLI

To modify an OSPF summary using the CLI, enter the following command in **Configure** mode:

```
cajun(configure router: ospf)# area <area-id>
range <ip-address> <mask>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Monitoring Switch Performance Using OSPF Statistics

You can monitor switch performance using the following OSPF statistics:

- OSPF Links
- OSPF Neighbors
- OSPF Link Database

Displaying OSPF Statistics

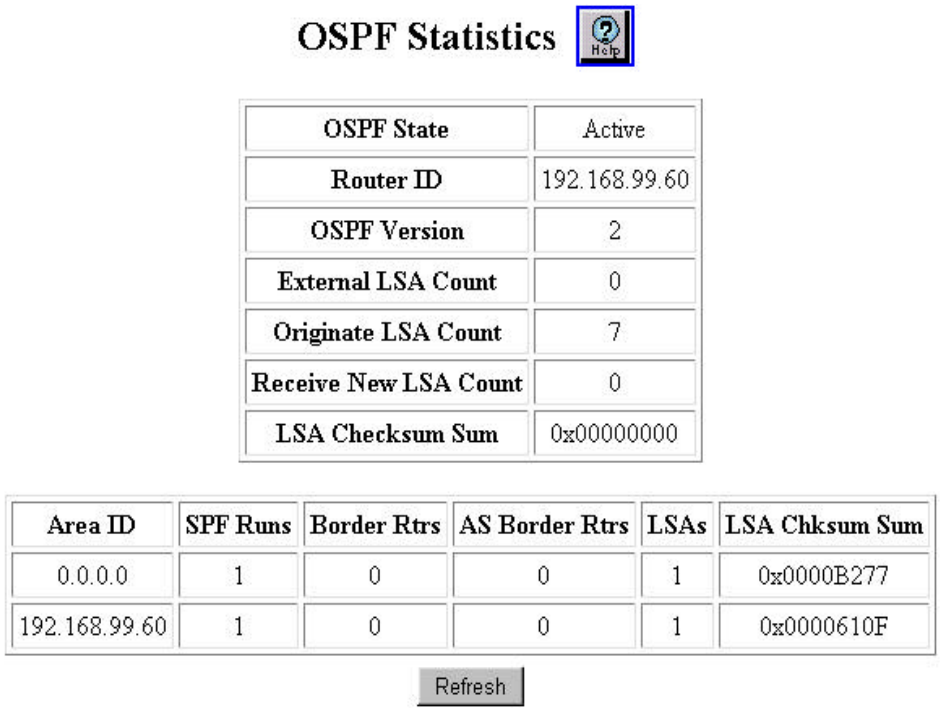
You can display OSPF statistics using either the web agent or the CLI.

Displaying OSPF Statistics Using the Web Agent

To display the OSPF global statistics using the web agent:

1. Select Statistics from the Routing > IP > OSPF group on the Web Agent window. The OSPF Statistics dialog box opens (Figure 11-9).

Figure 11-9. OSPF Statistics Dialog Box



2. Refer to Table 11-6 for an explanation of the OSPF Statistics dialog box parameters:

Table 11-6. OSPF Statistical Parameters

Parameter	Displays the...
OSPF State	Current state of OSPF.
Router ID	Router ID for OSPF.
OSPF Version	Current version of OSPF. The P550 with Integrated Routing supports OSPFv2.
External LSA Count	Number of external (LS type 5) link state advertisements (LSAs) in the link-state database.
Originate LSA Count	Number of LSAs originated by this router.
Receive New LSA Count	Number of new LSAs received by this router.
LSA Checksum Sum (global OSPF system)	32-bit unsigned sum of the LS checksums of the external link-state advertisements contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.

Table 11-6. OSPF Statistical Parameters continued

Parameter	Displays the...
Area ID	Area ID of the area in question. It has the function of defining a summarization point for Link State Advertisements.
SPF Runs	Number of times that the intra-area route table has been calculated using this area's link-state database.
Border Rtrs	Total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
AS Border Rtrs	Total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
LSAs	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
LSA Chksum Sum (per area, not globally)	32-bit unsigned sum of the LS checksums of the external link-state advertisements contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.

3. Click Refresh to reset the counters with the latest information.

Displaying OSPF Statistics Using the CLI

To display the OSPF global statistics using the CLI, enter the following command in Priv mode:

```
cajun# show ip ospf stats
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying OSPF Links

The OSPF link display provides information on the currently active OSPF links. You can display the OSPF using either the web agent or the CLI.

Displaying OSPF Links Using the Web Agent

To display OSPF links using the web agent:

1. Select Links from the Routing > IP > OSPF group on the web agent window. The OSPF Links dialog box opens (Figure 11-10).

Figure 11-10. OSPF Links Dialog Box

OSPF Links

State	IP Address	Area ID	Type	DR Router ID	DR Address	BDR Address
UP	192.168.99.60	192.168.99.60	Ethernet LAN	192.168.99.60	192.168.99.60	0.0.0.0
DOWN	0.0.0.0	192.168.99.60	Virtual Link	n/a	n/a	n/a

2. Refer to Table 11-7 for an explanation of the **OSPF Links** dialog box parameters:

Table 11-7. OSPF Link Parameters

Parameter	Displays the...
State	State of the OSPF link.
IP Address	IP address of the OSPF link.
Area ID	Area ID (IP address) associated with the OSPF link.
Type	Type of OSPF link.
DR Router ID	Router ID of the designated router.
DR Address	IP address of the designated router.
BDR Address	IP address of the designated border router.

Displaying OSPF Links Using the CLI

To display OSPF links using the CLI, enter the following command from Priv mode:

```
cajun# show ip ospf virtual-links
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying OSPF Neighbors

The OSPF neighbors table summarizes the list of OSPF interfaces and their associated neighbors. You can display OSPF neighbors using either the web agent or the CLI.

Displaying OSPF Neighbors Using the Web Agent

To display the OSPF neighbors using the web agent:

1. Select Neighbors from the Routing > IP > OSPF group on the web agent window. The OSPF Neighbors dialog box opens (Figure 11-11).

Figure 11-11. OSPF Neighbors Dialog Box

OSPF Neighbors

IP Address	State	Router ID	Master	DD Number	DR Priority	E-Option	T-Option	MC-Option	N-Option	OPQ-Option	DR Choice	BDR Choice
15.0.7.1	FULL	15.0.7.1	Slave	0x00001107	1	Yes	No	No	No	No	15.0.7.1	15.0.7.2
15.0.21.2	FULL	15.0.21.2	Master	0x0000161A	1	Yes	No	No	No	No	15.0.21.2	15.0.21.1

2. Refer to Table 11-8 to review the OSPF neighbors parameters:

Table 11-8. OSPF Neighbors Parameters

Parameter	Definition
IP Address	The IP address associated with the OSPF neighbor.
State	The functional level of an interface. States include: • **Down** - This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor. • **Attempt** - Indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor • **INIT** - Indicates that the Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor. • **2-Way** - Communication between the two routers is bidirectional. • **ExStart** - This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial Database Description sequence number. Neighbor conversations in this state or greater are called adjacencies. • **Exchange** - Router is describing its entire link state database by sending DD (Database Description) packets to the neighbor. • **Loading** - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • **Full** - The neighboring routers are fully adjacent. These adjacencies appears in router-LSAs and network-LSAs.
Router ID	The router ID of the neighbor.
Master	The state of the neighbor: master or slave.
DD Number	The hexadecimal number used to sequence the collection of Database Description Packets. The initial value (indicated by the Init bit being set) should be unique. The DD sequence number then increments until the complete database description has been sent.

Table 11-8. OSPF Neighbors Parameters continued

Parameter	Definition
DR Priority	Displays the DR Priority of the neighboring router. This is used to determine whether this neighbor is eligible to become the *Backup* Designated Router. If 0, the router is ineligible to become the Backup Designated Router.
E-Option	The method used to flood AS-external-LSAs.
T-Option	Specifies whether this neighbor is an ASBR.
MC-Option	Specifies whether this neighbor supports MOSPF.
N-Option	Specifies whether this neighbor supports the handling of Type-7 LSAs.
OPQ-Option	Specifies whether this neighbor supports opaque LSAs (LSA type 9-11).
DR Choice	Interface IP address of the designated router.
BDR Choice	Interface IP address of the backup designated router.

Displaying OSPF Neighbors Using the CLI

To display the OSPF neighbors using the CLI, enter the following command in Priv mode:

```
cajun# show ip ospf neighbor
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Searching the OSPF Link State Database

You can search the OSPF kink state database using either the web agent or the CLI.

Searching the OSPF Link State Database Using the Web Agent

To search the OSPF link state database using the web agent:

1. Select Link State Database Search from the Routing > IP > OSPF group on the web agent window. The Link State Database Search dialog box opens (Figure 11-12).

   Note: You can select more than one item in the Search By column to help narrow your search results.

Figure 11-12. Link State Database Search Dialog Box

OSPF Link State Database

Detail Link	Area ID	Type	LS ID	Router ID	Sequence	Age	Checksum
Details	192.168.99.60	Router Links	192.168.99.60	192.168.99.60	0x8000000A	1284	0x5515

2. To search by:

   — **Area ID** — click the Area ID checkbox and specify the IP address of the Area ID that you want to find in the database, and click SEARCH.

   — **Type** — click the Type checkbox and from the Type pull-down menu, select the type of search you want to perform, and click SEARCH.

   — **Router ID** — click the Router ID checkbox and specify the router IP address, and click SEARCH.

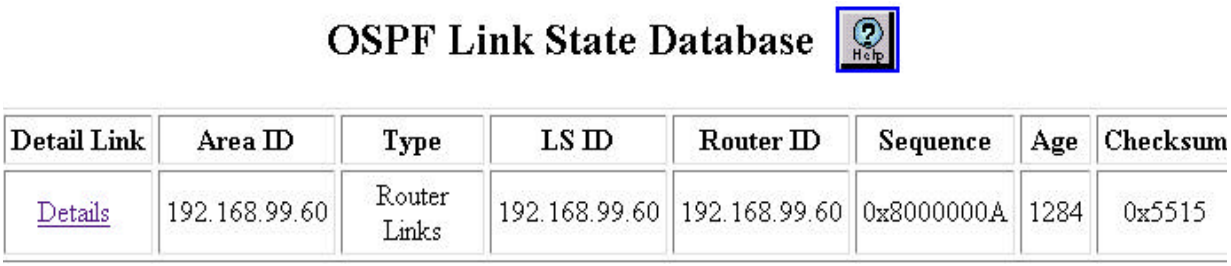
3. Refer to Table 11-9 for an explanation of the OSPF Link State Database Search dialog box parameters:

Table 11-9. OSPF Link State Database Search Dialog Box Parameters

Parameter	Allows you to ...
Area ID	search for the 32-bit identifier of the area from which a LSA was received.
Type	search for all entries in the database that match one of the following types: • **Router Links** - These packets describe the states of the router's links to the area and are only flooded within a particular area. • **Network Links** - These packets are generated by Designated Routers and describe the set of routers attached to a particular network. • **Summary Network** - These summaries are generated by Area Border Routers and describe inter-area routes to various networks. They can also be used for aggregating routes. • **Summary AS border** - This describes links to Autonomous System Border Routers and are generated by Area Border Routers. • **AS external** - These packets are generated by Autonomous System Border Routers and describe routes to destination external to the Autonomous system. They are flooded everywhere except stub areas. • **Multicast group** - These packets are generated by multicast groups. • **NSSA external** - These packets are generated by Area Border Routers and describe routes within the NSSA (Not-So-Stubby-Area).
Router ID	search of the link state database for entries originated by this router.

4. **If your search produces results, the detailed information displays in the OSPF Link State Database dialog box (Figure 11-13).**

Figure 11-13. OSPF Link State Database Dialog Box



5. Refer to Table 11-10 for an explanation of the OSPF Link State Database dialog box parameters.

Table 11-10. OSPF Link State Database Parameters

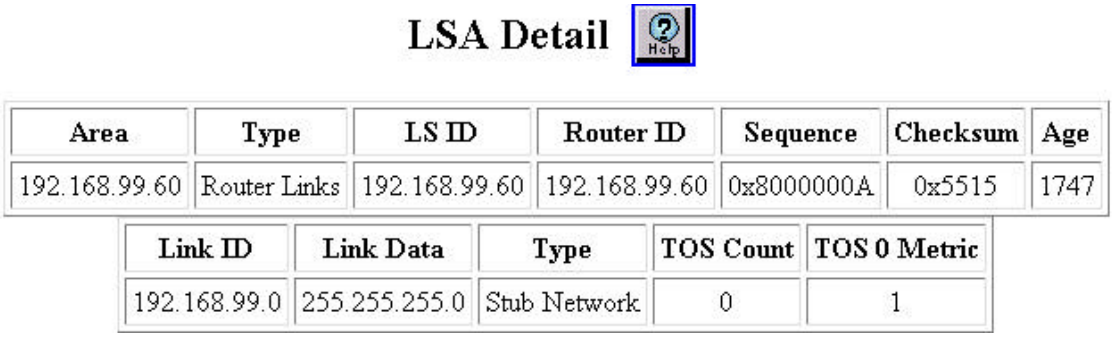
Parameter	Displays ...
Detail Link	A link to the LSA Detail dialog box.
Area ID	The 32-bit identifier of the area from which the LSA was received.
Type	The LSA format and function. Types include: • **Router Links** - These packets describe the states of the router's links to the area and are only flooded within a particular area. • **Network Links** - These packets are generated by Designated Routers and describe the set of routers attached to a particular network. • **Summary Network** - These summaries are generated by Area Border Routers and describe inter-area routes to various networks. They can also be used for aggregating routes. • **Summary AS Border** - This describes links to Autonomous System Border Routers and are generated by Area Border Routers. • **AS External** - These packets are generated by Autonomous System Border Routers and describe routes to destinations external to the Autonomous system. They are flooded everywhere except stub areas. • **Multicast Group** - These packets are generated by multicast groups. • **NSSA External** - These packets are generated by Area Border Routers and describe routes within the NSSA (Not-So-Stubby-Area).

Table 11-10. OSPF Link State Database Parameters continued

Parameter	Displays ...
LS ID	The piece of routing domain that is being described by the advertisement. Depending on the advertisements LS type, the LS ID displays different values.
Router ID	The 32-bit number that uniquely identifies the originating router in the Autonomous System.
Sequence	The sequence number.
Age	Displays the age (in seconds) of the LSA.
Checksum	Displays the checksum of the complete contents of the advertisement, except the age field.

6. Select Details from the Detail Link column to display more OSPF link state database search results. The LSA Details dialog box displays with additional search information (Figure 11-14).

Figure 11-14. LSA Detail Dialog Box



7. Refer to Table 11-11 for an explanation of the LSA Detail dialog box parameters.

Table 11-11. LSA Detail Dialog Box Parameters

Parameter	Definition
Area	Displays the 32-bit identifier of the area from which the LSA was received.
Type	Displays the link state type. Types include: • Router Links • Network Links • Summary Network • Summary AS Border • AS External • Multicast Group • **NSSA External**
LS ID	Displays the link-state ID. The link-state ID is an LS type specific field containing either a router ID or an IP address that identifies the piece of the routing domain that is being described by the advertisement.
Router ID	Displays the router ID of the originator of the link state advertisement.
Sequence	Displays the link-state sequence number. The sequence number is a 32-bit signed integer.
Checksum	Displays the checksum of the complete contents of the advertisement, except the age field.
Age	Displays the time (in seconds) of the LSA.
Link ID	Displays the neighboring router's interface ID.
Link Data	Displays the interface ID of the associated router interface.
Type	Displays the link type of Router Network LSAs. Types include: • Point-to-point Link (1) • Transit Network (2) • Stub Network (3) • Virtual Link (4)
TOS Count	Displays the type-of-service count.
TOS 0 Metric	Displays the type-of-service cost of the interface.
Network Mask	Displays the network mask for the LSA.

***Table 11-11. LSA Detail Dialog Box Parameters** continued*

Parameter	Definition
External	Displays whether the route is connected to an external network. This parameter is associated with AS External LSAs.
TOS	Displays the type-of-service of the route. This parameter is associated with AS External, Summary Network, and Summary AS Border LSAs.
Metric	Displays the cost of the link. This parameter is associated with AS External, Summary Network, and Summary AS Border LSAs.
Forward Address	Displays the forward address. This indicates that packets for the external destination should be forwarded to the advertising OSPF router. This parameter is associated with AS External LSAs.
Tag	Displays the tag associated with the LSA. This parameter is associated with AS External LSAs.
Attached Router ID 1 &2	Displays the router ID for the attached router(s).

Searching the OSPF Link State Database Using the CLI

To search the OSPF link state database using the CLI, enter the following command from Priv mode:

```
cajun# show ip ospf database <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

12 Configuring IPX Routing

Overview

This chapter provides the following information and procedures for configuring layer 3 modules:

- Internetwork Packet Exchange (IPX) Protocol Overview
- Configuring the Cajun Switch as an IPX Router

Internetwork Packet Exchange (IPX) Protocol Overview

The IPX protocol is connectionless and performs datagram delivery and routing in Novell NetWare networks. Each IPX address consists of:

- **Network Number** — A 32-bit (8 characters) number that is normally assigned by the network administrator.
- **Node Number** — A 48-bit (12 characters) number that is normally the MAC layer address of the physical interface.
- **Socket Number** — A number used to route packets to different processes within the same node.

The syntax for entering an IPX address is:

```
network node socket
```

For example:

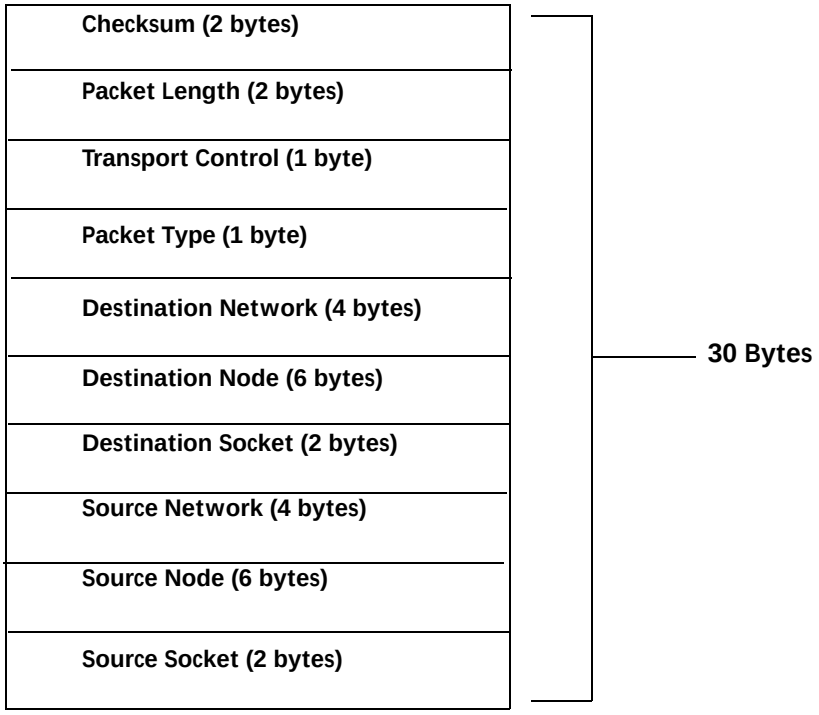
```
000000AAh 00e03b124213h 4003h
```

where `000000AAh` is the network number, `00e03b124213h` is the node number, and `4003h` is the socket number associated with a running process on the end node (for example, RIP, NetWare Link State Protocol (NLSP)).

IPX Datagram Structure

The IPX datagram contains an IPX header and any data to be transferred on the network. The IPX header is a 30 byte header that contains 10 fields. Figure 12-1 illustrates a conceptual view of an IPX datagram:

Figure 12-1. IPX Datagram in Detail



Refer to Table 12-1 for a description of the IPX datagram Structure fields:

Table 12-1. IPX Datagram Structure Fields

Field	Definition
Checksum	Provides integrity checking. **Note:** Checksum is normally *not enabled* in IPX networks and is usually set to 0xFFFF.
Packet Length	Length (in bytes) of the packet.
Transport Control	Number of routers a packet has traversed. This is used to discard a packet if the packet traverses a maximum number of routers (16).
Packet Type	Indicates the type of service required or offered by the packet. Types include: • Sequenced Packet Exchange (SPX packet) • NetWare Core Protocol (NCP packet) • NetBIOS (propagated packet)
Destination Network	The IPX network address of the destination network.
Destination Node	The MAC address of the destination node.
Destination Socket	Address of the process running in the destination node. Sockets route packets to different processes within the same node.
Source Network	The network address of the source network.
Source Node	The MAC address of the source node.
Source Socket	Address of the process running in the source node.

Configuring the Cajun Switch as an IPX Router

You can configure the Cajun P550/P880/P882 switch as an IPX router. Specific hardware is required to accomplish this configuration.

Hardware Requirements

To configure your switch as an IPX router, your Cajun P550/P880/P882 switch must be configured with the following hardware:

- Layer 3 supervisor module
- Layer 3 media modules (optional) including:
  - 2-Port Gigabit Ethernet module
  - 10-Port 100-Base-F module
  - 12-Port 10/100-Base-T module

Configuring IPX Routing Globally

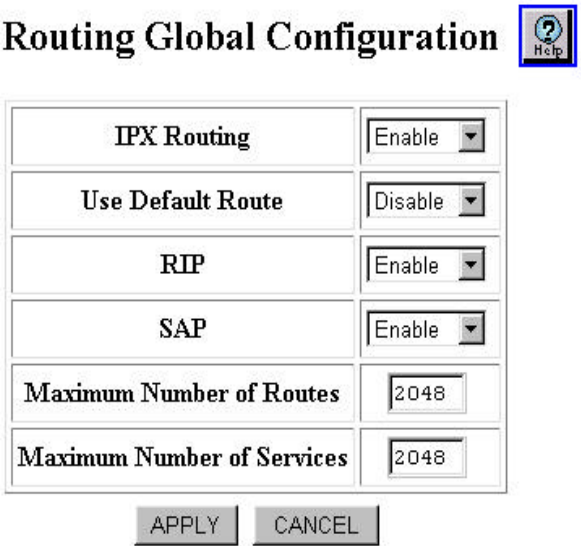
You can configure IPX routing globally using the web agent or the CLI.

Configuring IPX Routing Globally Using the Web Agent

To configure IPX routing globally using the web agent:

1. Select Global Configuration from the Routing > IPX > Configuration group on the web agent window. The IPX Global Configuration dialog box opens (Figure 12-2).

Figure 12-2. IPX Global Configuration Dialog Box



2. Configure IPX Routing Global Configuration dialog box parameters to make your switch an IPX router. Refer to Table Table 12-2 for an explanation of the dialog box parameters.

Table 12-2. IPX Routing Global Configuration Dialog Box Parameters

Parameter	Allows you to ...
IPX Routing	Select Disable to prevent IPX from routing globally. The default value is Enable.
Use Default Route	Select Enable if you know the default route. The default value is Disable.
RIP	Select Disable to prevent IPX RIP from routing globally. This affects all IPX interfaces set up to use the IPX RIP routing protocol. The default value is Enable.
SAP	Select Disable to prevent IPX SAP from routing globally. This affects all IPX interfaces set up to use the IPX SAP routing protocol. The default value is Enable.
Maximum Number of Routes	Enter the maximum number of routes that can be added to the routing table. The switch rounds your entry to the nearest power of 2. For example, if you enter 1000, the system rounds this number up to 1024 routes. The default value is 2048.
Maximum Number of Services	Enter the maximum number of services that can be added. The switch rounds your entry to the nearest power of 2. For example, if you enter 1000, the system rounds this number up to 1024 services. The default value is 2048.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring IPX Routing Globally Using the CLI

To configure IPX routing globally using the CLI, enter the following command from Configure mode:

```
cajun(configure)# ipx rip
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring IPX Interfaces

You can create new IPX interfaces and configure up to four interfaces of different encapsulation types to a VLAN (multinetting). You can configure an IPx interface using either the web agent or the CLI.

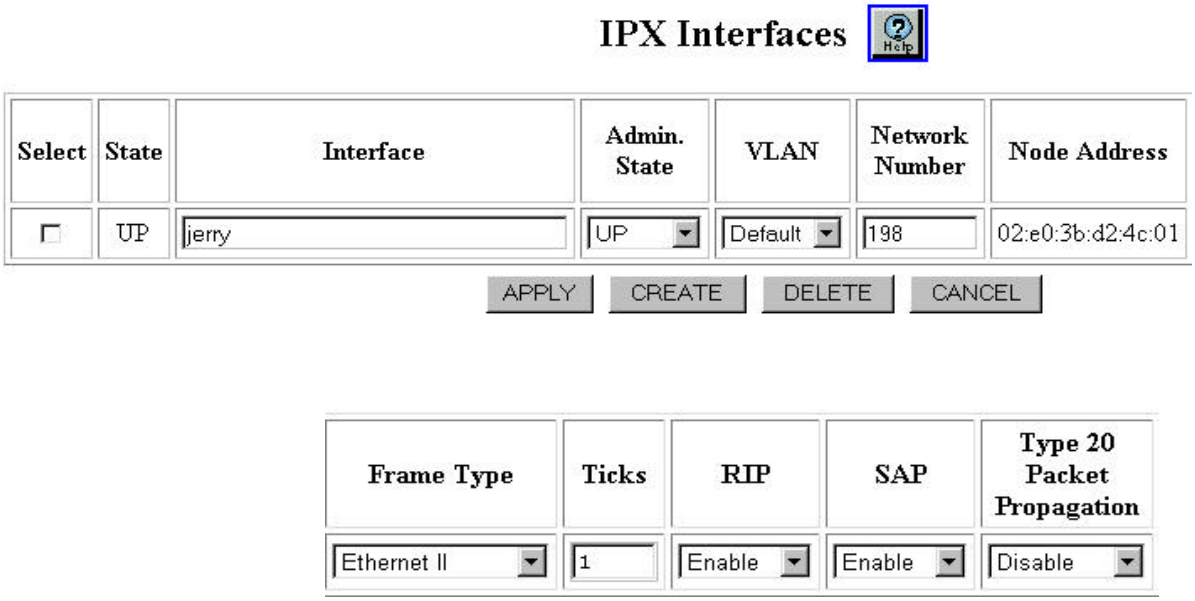
Configuring an IPX Interface Using the Web Agent

To create a new IPX interface using the web agent:

1. Select Interfaces from Routing > IPX > Configuration group on the web agent window. The IPX Interfaces dialog box opens (Figure 12-3).

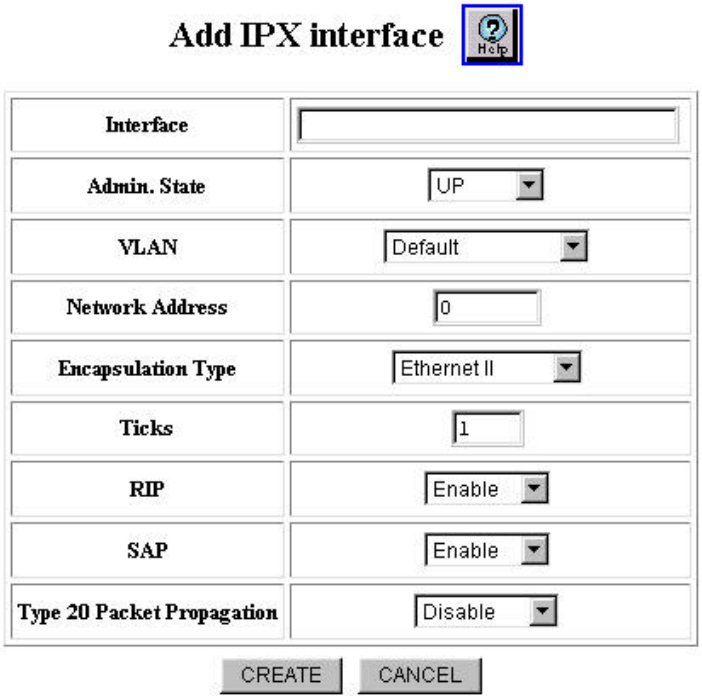
   ***Note:** Due to its length, the **IPX Interfaces** dialog box is split into two views.

Figure 12-3. IPX Interfaces Dialog Box



2. Select **CREATE**. The **Add IPX Interface** dialog box opens (see Figure 12-4).

Figure 12-4. Add IPX Interface Dialog Box



3. Select the VLAN to which you want to assign an IPX network address from the VLAN pull-down menu.

***Note:** If you need to create a new VLAN, refer to *"Creating and Implementing VLANs"* in Chapter 4.

4. Refer to Table 12-3 to configure an IPX interface:.

Table 12-3. IPX Interface Dialog Box Parameters

Parameter	Allows you to...
Select	Select the interface to be configured. This field is displayed in the IPX Interfaces Dialog box not in the Add IPX Interface dialog box, and only if IPX interfaces have been created previously.
State	Displays the current state of the interface. The state options are: **Up** **Down** The State is displayed in the IPX Interfaces dialog box, not in the Add IPX Interface dialog box.
Interface	Enter the name of the IPX interface.

***Table 12-3. IPX Interface Dialog Box Parameters** continued*

Parameter	Allows you to...
Admin. State	Select the administration state of the interface. Options include: Up Down
VLAN	Select the VLAN that corresponds to the IPX interface you selected.
Network Address	Enter the number of the IPX network you want to assign to the IPX interface. This number is a hexadecimal number.
Node Address	Displays the node address on which the IPX interface resides. This parameter is displayed in the IPX Interface dialog box, not in the Add IPX Interface dialog box.
Frame Type	Select the format of the MAC header on the IPX packets sent by the router on the interface. Formats include: **Ethernet II** (Maximum Transmission Unit (MTU) = 1500) **Ethernet 802.2** (MTU = 1497) **Ethernet SNAP** (MTU = 1492) **Ethernet 802.3** (MTU = 1500)
Ticks	Specify the amount of time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second.
RIP	Select Disable to prevent IPX RIP from routing globally. This affects all IPX interfaces set up to use the IPX RIP routing protocol. The default value is Enable.
SAP	Select **Disable** to prevent IPX SAP from routing globally. This affects all IPX interfaces set up to use the IPX SAP routing protocol. The default value is **Enable**.
Type 20 Packet Propagation	Specify whether or not Type 20 packets can be sent, received, disabled, or sent and received on a given interface. Options include: **Disable** - Type 20 packets are neither sent nor received. **Inbound** - Type 20 packets are received. **Outbound** - Type 20 packets are sent. **Both** - Type 20 packets are sent and received.

5. Click **CREATE** to save your changes or **CANCEL** to restore previous settings.

Configuring an IPX Interface Using the CLI

To create a new IPX interface using the CLI, enter the following command in Configure mode:

```
cajun(configure)# interface <interface name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating IPX Static Routes

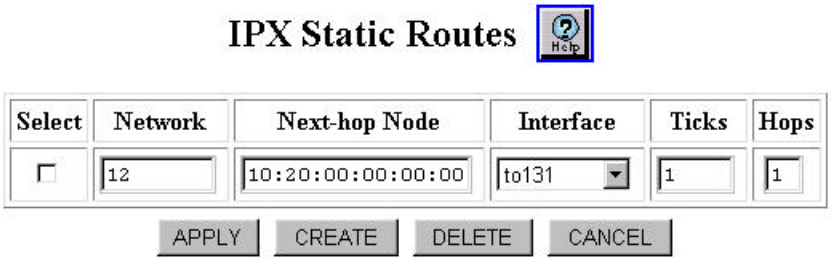
You can create IPX static routes using either the web agent or the CLI.

Creating IPX Static Routes Using the Web Agent

To create IPX static routes using the web agent:

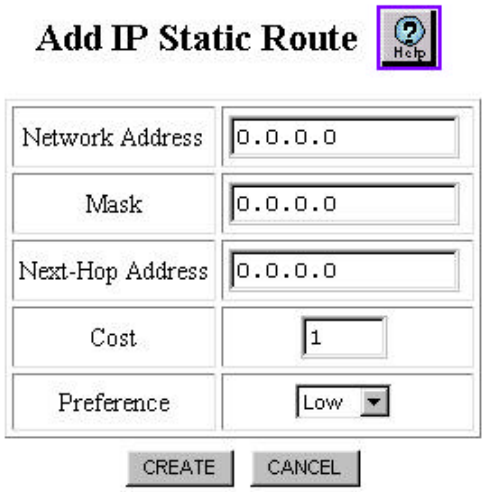
1. Select Static Routes from Routing > IPX > Configuration group on the web agent window. The IPX Static Routes dialog box opens (see Figure 12-3).

Figure 12-5. IPX Static Routes Dialog Box.



2. Select CREATE. The Add IPX Static Route dialog box opens (see Figure 12-6).

Figure 12-6. Add IPX Static Route Dialog Box



3. Refer to Table 12-4 to configure the IPX Static Route parameters.

Table 12-4. IPX Static Route Parameters

Parameter	Allows you to ...
Network	Enter the IPX network number that you want to assign to the IPX static route.
Next-Hop Node	Enter the MAC address for the next destination to which the packet is routed. Format of the value to enter is **aa:bb:cc:dd:ee:ff**.
Interface	View the IPX Interface associated with the next hop.
Ticks	Enter the amount of time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second.
Hops	Enter the number of routers (hops) that the packet must pass through before reaching the network number associated with the IPX network.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating IPX Static Routes Using the CLI

To create IPX static routes using the CLI, enter the following command in Interface mode:

```
cajun(configure if-<if-name>: ipx route <network
address|range> <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting IPX Static Routes

You can delete an IPX static route using either the web agent or the CLI.

Deleting IPX Static Routes Using the Web Agent

To delete an IPX static route using the web agent:

1. Select Static Routes from the Routing > IPX > Configuration group on the web agent window. The IPX Static Routes dialog box opens (see Figure 12-5).
2. Select the checkbox for the IPX static route that you want to delete from the Select column.
3. Click DELETE to remove the IPX static route, or CANCEL to restore the IPX static route.

Deleting IPX Static Routes Using the CLI

To delete an IPX static route using the CLI, enter the following command from Configure mode:

```
cajun(configure)# clear ipx route {<network>
default|*}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying IPX Static Routes

You can modify IPX static routes form either the web agent or the CLI.

Modifying IPX Static Routes Using the Web Agent

To modify an IPX static route using the web agent:

1. Select Static Routes from the Routing > IPX > Configuration group on the web agent window. The IPX Static Routes dialog box opens (see Figure 12-5).
2. Select the checkbox for the IPX static route that you want to modify from the Select column.
3. Refer to Table 12-4 to modify the IPX Static Route configuration.
4. Click APPLY to save your changes, or CANCEL to restore previous settings.

Modifying IPX Static Routes Using the CLI

To modify an IPX static route using the CLI, enter the following command Interface mode:

```
cajun(configure if-<if-name>)# ipx route <network
address|range> <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating IPX Static Services

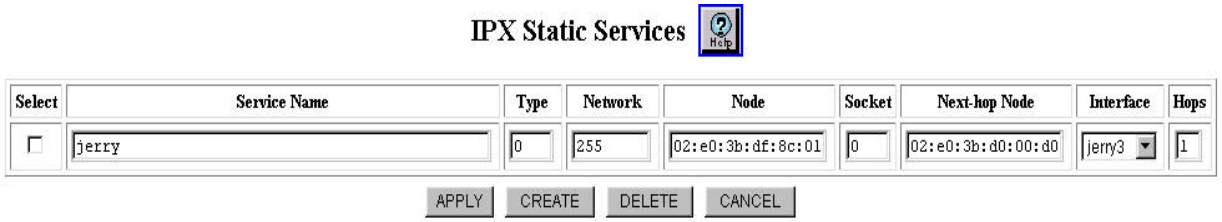
You can create IPX static services using either the web agent or the CLI.

Creating IPX Static Services Using the Web Agent

To create IPX static services using the web agent:

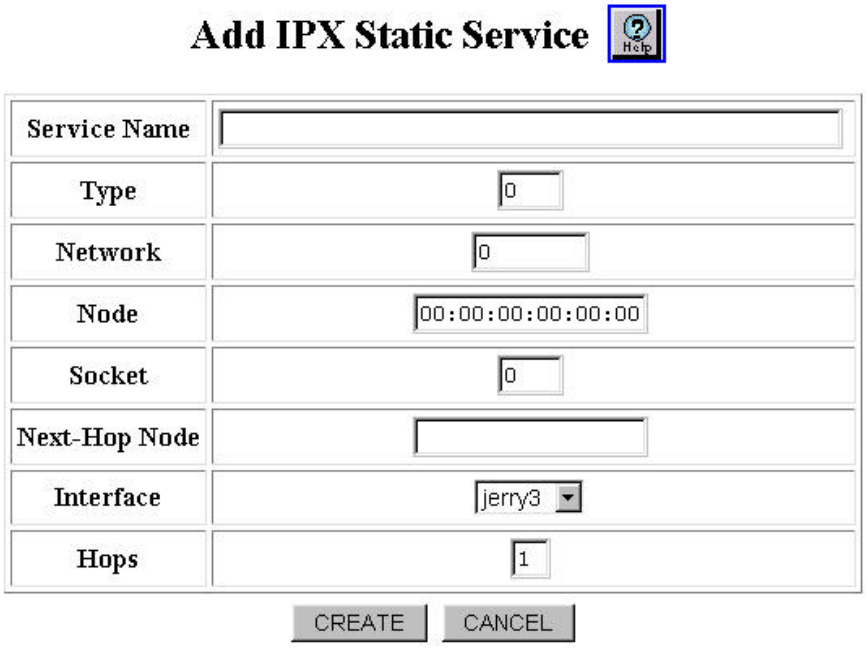
1. Select Static Services from the Routing > IPX > Configuration group on the web agent window. The IPX Static Services dialog box opens (see Figure 12-7).

Figure 12-7. IPX Static Services Dialog Box



2. Select CREATE to create a new static service. The Add IPX Static Service dialog box opens (see Figure 12-8).

Figure 12-8. Add IPX Static Service Dialog Box



3. Refer to Table 12-5 to configure the Add IPX Static Service dialog box parameters.:

Table 12-5. IPX Static Service Dialog Box Parameters

Parameter	Allows you to ...
Service Name	Enter the IPX Static Service name. For example, FS_ENG01. Use SLIST (NetWare 3.x) or NLIST (NetWare 4.x) to list your current server names and types from your NetWare server.
Type	Enter the service type (in hex) that identifies the type of IPX static service the server provides. Well-known service types include: • Unknown (0) • Print Queue (3) • File Server (4) • Job Server (5) • Print Server (7) • Archive Server (9) • Remote Bridge Server (24) • Advertising Print Server (47)
Network	Enter the IPX Static Service network number.
Node	Enter the IPX Static Service node address (in hex). The format of the node value is **aa:bb:cc:dd:ee:ff**.
Socket	Enter the number (in hex) associated with a running process on the end node (for example, RIP, NLSP).
Next-Hop Node	Enter the MAC address of the next destination through which the service is reached. The format of the node value is **aa:bb:cc:dd:ee:ff**.
Interface	Enter the interface that corresponds to the next-hop node.
Hops	Enter the number of routers (hops) that the packet must pass through before reaching the network number associated with the service.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating IPX Static Services Using the CLI

To create IPX static services using the CLI, enter the following command in Priv mode:

```
cajun# ipx service <service-type type |range>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting IPX Static Service

You can delete an IPX static service using wither the web agent or the CLI.

Deleting IPX Static Service Using the Web Agent

To delete an IPX static service using the web agent:

1. Select Static Services from the Routing > IPX > Configuration group on the web agent window. The IPX Static Services dialog box opens (see Figure 12-7).
2. Select the IPX Static Service that you want to remove.
3. Click DELETE to remove the IPX static service, or CANCEL to keep the IPX Static Service.

Deleting IPX Static Service Using the CLI

To delete an IPX static service using the CLI, enter the following command in Priv mode:

```
cajun(configure)# clear ipx service {<service-
type> <service-name>|*}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying IPX Static Service

You can modify an IPX static service using either the web agent or the CLI.

Modifying IPX Static Service Using the Web Agent

To modify an IPX static service using the web agent:

1. Select Static Services from the Routing > IPX > Configuration group on the web agent window. The IPX Static Services dialog box opens (see Figure 12-7).
2. Select the checkbox for the IPX Static Service that you want to modify from the Select column.
3. Refer to Table 12-5 to modify the IPX Static Services dialog box parameters.

Modifying IPX Static Service Using the CLI

To modify an IPX static service using the CLI, enter the following command in Priv mode:

```
cajun(configure)# ipx service <service-type>
<service-name> <network> <node> <socket>
<network.next-hop-node> <hops>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Monitoring Your Switch Using IPX

This section explains how to use IPX to do the following on your switch:

- Examine IPX Global Statistics
- Search the IPX Route Table
- Examine the IPX Route Table
- Examine IPX Route Table Statistics
- Search the IPX Service Table
- Examine the IPX Service Table
- Examine IPX Service Table Statistics

Examine IPX Global Statistics

IPX Global Statistics count only the IPX packets that are received by or sent from the Supervisor module, not those packets routed in hardware.

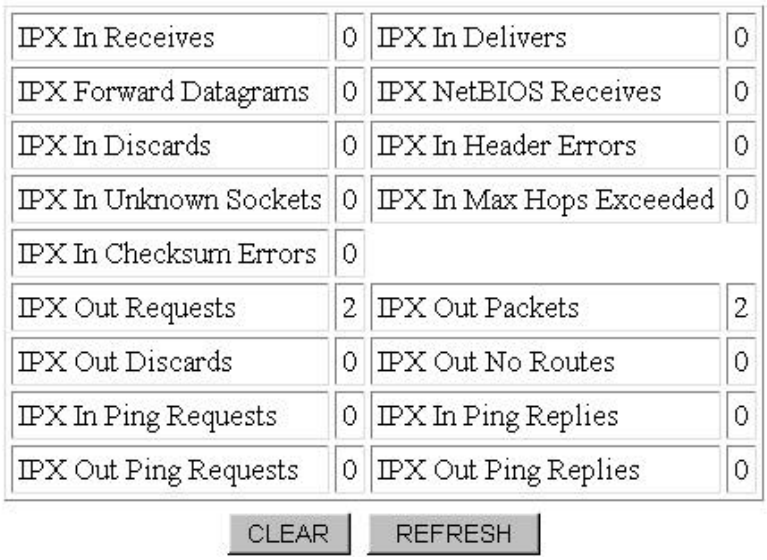
You can examine the IPX Global statistics using either the web agent or the CLI.

Examine IPX Global Statistic Using the Web Agent

To examine the global IPX routing statistics using the web agent:

1. Select Global Statistics from the Routing > IPX > Display group on the Web Agent window. The IPX Routing Global Statistics dialog box opens (see Figure 12-9).

Figure 12-9. IPX Global Statistics Dialogue Box


IPX Global Statistics
Help
IPX In Receives 0
IPX In Delivers 0
IPX Forward Datagrams 0
IPX NetBIOS Receives 0
IPX In Discards 0
IPX In Header Errors 0
IPX In Unknown Sockets 0
IPX In Max Hops Exceeded 0
IPX In Checksum Errors 0
IPX Out Requests 2
IPX Out Packets 2
IPX Out Discards 0
IPX Out No Routes 0
IPX In Ping Requests 0
IPX In Ping Replies 0
IPX Out Ping Requests 0
IPX Out Ping Replies 0
CLEAR
REFRESH

2. To view the latest statistics available, click REFRESH to update all statistics.

3. To reset all of the statistics that are currently displayed, click CLEAR. The statistics all reset to zero.

4. Refer to Table 12-6 for a explanation of the IPX Global Statistics dialog box parameters:

Table 12-6. IPX Global Statistics Dialogue Box Parameters

Parameter	Allows you to...
IPX In Receives	View the total number of IPX packets received (including errors).
IPX In Delivers	View the total number of IPX packets delivered locally. This includes packets from local applications.
IPX Forward Datagrams	View the number of IPX packets forwarded.
IPX Netbios Receives	View the number of NetBIOS packets received.
IPX In Discards	View the number of IPX packets received but discarded.
IPX In Header Errors	View the number of IPX packets discarded because of errors in the packet header. This includes packets that are less than the minimum 30 byte length.
IPX In Unknown Sockets	View the number of IPX packets discarded because the destination socket was not open.

Table 12-6. IPX Global Statistics Dialogue Box Parameters continued

Parameter	Allows you to...
IPX In Max Hops Exceeded	View the number of IPX packets discarded because the Transport Control field is greater than or equal to 16.
IPX In Checksum Errors	View the number of IPX packets received with bad checksums.
IPX Out Requests	View the number of IPX packets supplied locally for transmission. This does not include any packets counted in IPX Forward Datagrams.
IPX Out Packets	View the total number of IPX packets transmitted.
IPX Out Discards	View the number of outgoing IPX packets discarded.
IPX Out No Routes	View the number of IPX packets that cannot be transmitted because no routes are available.
IPX In Ping Requests	View the number of received ping requests.
IPX In PingReplies	View the number of received replies made to ping requests.
IPX Out Ping Requests	View the number of transmitted ping requests.
IPX Out Ping Replies	View the number of transmitted replies made to ping requests.

Examine IPX Global Statistic Using the CLI

To examine the global IPX routing statistics using the CLI, enter the following command from Priv mode:

```
cajun# show ipx route
```

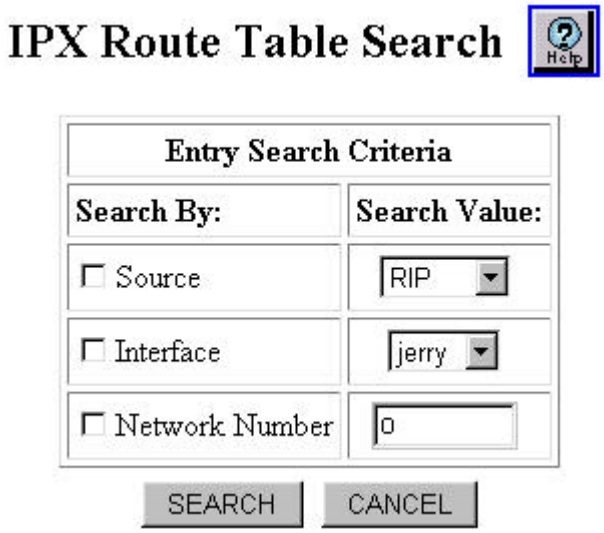
Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Search the IPX Route Table

To search the IPX route table:

1. Select Route Table Search from the Routing > IPX > Display web agent window. The IPX Route Table Search dialog box opens (see Figure 12-10).

Figure 12-10. IPX Route Table Search Dialog Box



2. Select the Search Criteria you want to use to find information on specific routes. For example, if you want to find all static routes that are presently configured on your switch, search by source and specify static as your search value.

3. Refer to Table 12-7 to determine the search parameters:

Table 12-7. IPX Route Table Search Parameters

Parameter	Allows you to ...
Source	Search the IPX route table using of the following parameters: • **RIP** - RIP routing updates • **Static** - User configuration • **Local** - Directly connected routes Once you select a parameter, you can search to find the routes associated with that parameter.
Interface	Search the IPX Route table using the interface associated with the next-hop to the IPX network.
Network Number	Search the IPX Route table using the IPX Network address (hexadecimal number) you specify.

4. Select Search to start:

   — If the available routes are found they are displayed in the IPX Route Table dialog box.

   — If no routes are available, a message is displayed in the IPX Route Table dialog box.

Examine the IPX Route Table

To examine the IPX route table:

1. Perform an IPX Route Table search as described in "Search the IPX Route Table", section. If available routes are found they are displayed in the IPX Route Table dialog box.

2. Refer to Table 12-8 to review your configuration:

Table 12-8. IPX Route Table Parameters

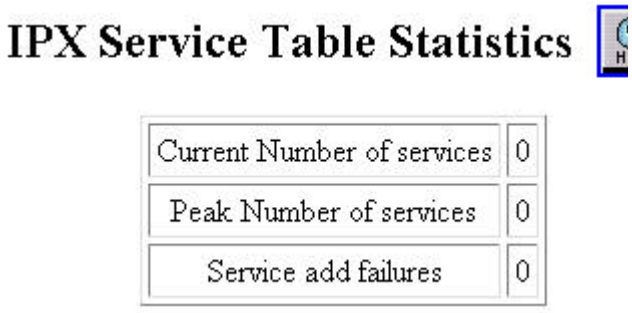
Parameter	Defines the...
Select	Parameter selected.
Network	Network number (in hex) of the IPX network.
Interface	Interface associated with the IPX network.
Source	Method by which the network was learned. For example, RIP, local, or static.
TTL	Number of seconds before the route expires.
Ticks	Amount of time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second.
Hops	Number of routers (hops) that the packet must pass through before reaching the network number associated with the IPX network.
Next-Hop MAC Address	MAC address of the next destination through which the network is reached.

Examine IPX Route Table Statistics

To examine your IPX route table statistics:

1. Select Route Table Statistics from the Routing > IPX > Display web agent window. The IPX Route Table Statistics dialog box opens (see Figure 12-11).

Figure 12-11. IPX Route Table Statistics Dialog Box



2. Refer to Table 12-9 and review each statistic:

Table 12-9. IPX Route Table Statistics

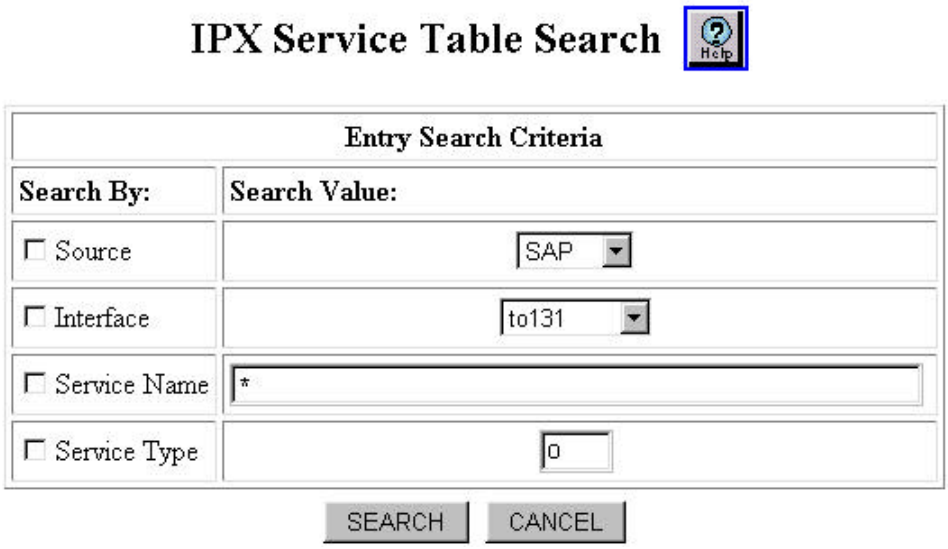
Statistic	Definition
Current Number of Routes	Indicates the current number of IPX routes.
Peak Number of Routes	Lists the peak number of routes.
Route Add Failures	Indicates the number of failed attempts to add a route to the routing table.

Search the IPX Service Table

To search the IPX service table:

1. Select Service Table Search from the Routing > IPX > Display web agent window. The IPX Service Table Search dialog box opens (see Figure 12-12).

Figure 12-12. IPX Service Table Search Dialog Box



2. Select the search criteria you want to use to find information on specific services in the Search By column. For example, if you want to find all static services that are presently configured on your switch, select Source from the Search By column and specify Static as your search value.

3. Refer to Table 12-10 to determine the search parameters:

Table 12-10. IPX Service Table Search Parameters

Parameter	Allows you to ...
Source	Search the IPX Service Table using one of the following parameters: • **SAP** - Services learned via the SAP protocol • **Static** - User configuration • **Local** - Local services Once you select a parameter, you can search to find the routes associated with that parameter.
Interface	Search the IPX Service Table using the interface associated with the next-hop to the service.
Service Name	Search the IPX Service Table using a service name you specify. Note that you can specify a single asterisk (*) to indicate a wildcard character that will match all characters entered before the wildcard. For example, entering FS_ENG* will find all service names that start with FS_ENG.
Service Type	Search the IPX Service Table using the service type you specify. For example, to specify a print queue type, you would enter 3 (0003h) in the space provided.

4. Click Search to start the search.

   — If available services are found they are displayed in IPX Service Table dialog box.

   — If services are not available, a message displays in the IPX Service Table dialog box.

Examine the IPX Service Table

To examine the IPX service table:

1. Perform an IPX Service table search as described in "Search the IPX Service Table", earlier in this chapter. If available services are found they are displayed in the IPX Service Table dialog box.

2. Refer to Table 12-11 to review each field in the IPX Services table:

Table 12-11. IPX Service Table Parameters

Parameter	Defines the...
Select	Parameter selected.
Name	Name of the service in question. For example, FS_ENG01. (Use SLIST (NetWare 3.x™) or NLIST (NetWare 4.x™) to list your current server names and types from your NetWare server.)
Type	Service type that identifies the type of service the server provides. Well known service types include: • Unknown (0) • Print Queue (3) • File Server (4) • Job Server (5) • Print Server (7) • Archive Server (9) • Remote Bridge Server (24) • Advertising Print Server (47)
Network	Network number of the IPX service.
Node	Node address of the service.
Socket	Number associated with a running process on the end node (for example, RIP, NLSP).
Interface	Interface associated with the next hop to the service.

Table 12-11. IPX Service Table Parameters continued

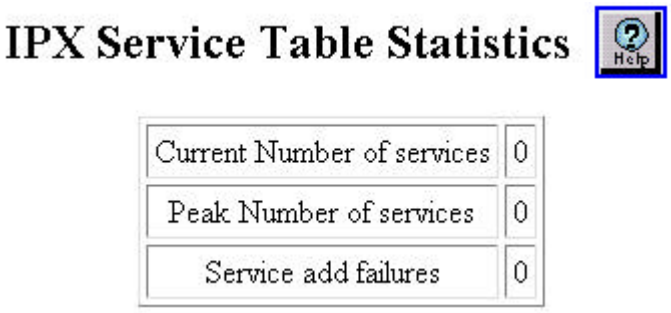
Parameter	Defines the...
Source	Method by which the service was learned. For example, SAP or static.
TTL	Number of seconds before the service expires.
Hops	Number of routers (hops) that the packet must pass through before reaching the network number associated with the service.
Next-Hop MAC Address	MAC address of the next destination through which the service is reached.

Examine IPX Service Table Statistics

To examine the IPX service table statistics:

1. Select Service Table Statistics from the Routing > IPX > Display web agent window. The IPX Service Table Statistics dialog box opens (Figure 12-13).

Figure 12-13. IPX Service Table Statistics



2. Refer to Table 12-12 to review each statistic:

Table 12-12. IPX Service Table Statistics Dialog Box

Statistic	Defines the...
Current Number of Services	The current number of IPX services.
Peak Number of Services	The peak number of services.
Service Add Failures	The number of failed attempts to add a service to the routing table.

13 Configuring IPX RIP Protocol

Overview

The information and procedures provided in this chapter pertain to layer 3 module configuration only. This chapter provides the following procedures:

- Configuring Internetwork Packet Exchange (IPX) Routing Interface Protocol (RIP) Interfaces
- Creating and Modifying IPX RIP Filters

Configuring Internetwork Packet Exchange (IPX) Routing Interface Protocol (RIP) Interfaces

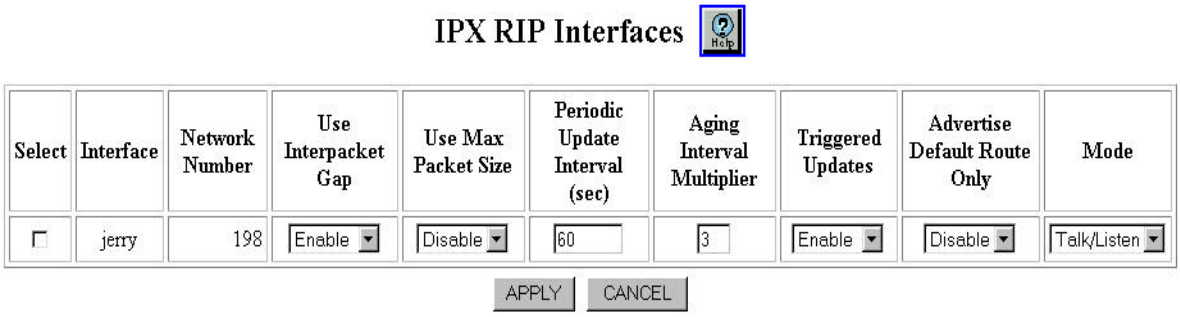
You can configure IPX RIP interfaces using either the web agent or the CLI.

Configuring IPX RIP Interfaces Using the Web Agent

To configure IPX RIP interfaces using the web agent:

1. Select Interfaces from the Routing > IPX > RIP group on the web agent window. The IPX RIP Interfaces dialog box opens (Figure 13-1)

Figure 13-1. IPX RIP Interfaces Dialog Box



2. Refer to Table 13-1 to modify the IPX RIP Interfaces dialog box parameters:

Table 13-1. IPX RIP Interfaces Dialog Box Parameters

Parameter	Allows you to...
Select	Select a RIP interface to modify. **Note:** This field is displayed in the IPX RIP Interface dialog box.
Interface	Identify the IPX interface associated with the RIP interface.
Network Number	Identify the number of the IPX network associated with the interface.
Use Interpacket Gap	Select **Disable** if you do not want RIP updates sent out over an interface to have an interpacket transmission delay. The default is **Enable**.
Use Max Packet Size	Enable or disable the transmission size of RIP packets sent out an interface: • **If** *enabled*, RIP packets can contain the maximum allowed by the MTU of the RIP interface. • **If** *disabled*, RIP packets are limited to 50 network entries.
Periodic Update Interval (sec)	Specify the length of time for the periodic update interval.
Aging Interval Multiplier	Specify the length of time that information from received RIP updates are kept as a multiplier of the Periodic Update Interval.
Triggered Updates	Select **Disable** to disallow RIP updates to be immediately transmitted to the network in response to changes in the network topology. The default is **Enable**.
Advertise Default Route Only	Select **Enable** to allow the advertising of the default network exclusively (subject to a route to the default network being known to the switch). The default is **Disable**.
Mode	Select the one of the following modes for the RIP interface: • **Talk/Listen** - Send and receive advertisements. • **Talk Only** - Send advertisements. • **Listen Only** - Receive advertisements.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring IPX RIP Interfaces Using the CLI

To configure IPX RIP interfaces using the CLI, enter the following command in Interface mode:

```
cajun(config-if: <if name>):# ipx rip
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating and Modifying IPX RIP Filters

You can create and modify IPX RIP filters from either the web agent or the CLI.

Creating and Modifying IPX RIP Filters Using the Web Agent

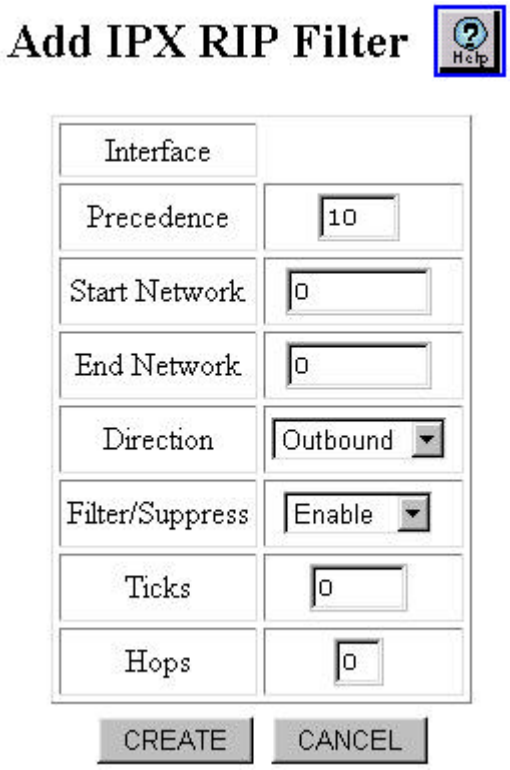
To create and modify IPX RIP filters using the web agent:

1. Select Filters from the Routing > IPX > RIP group on the Web Agent window. The IPX RIP Filters dialog box opens (Figure 13-2).

Figure 13-2. IPX RIP Filters Dialog Box

2. Select CREATE to create a new filter. The Add IPX RIP Filter dialog box opens (Figure 13-3).

Figure 13-3. Add IPX RIP Filter Dialog Box



3. Refer to Table 13-2 to modify the Add IPX RIP Filter dialog box parameters.:

Table 13-2. Add IPX RIP Filters Dialog Box Parameters

Parameter	Allows you to...
Interface	Select the interface to which this filter will be applied to RIP packets sent and/or received on the interface.
Precedence	Specify the filter precedence (in order of importance) with 0 equal to most important. **Note:** All filters on the same interface, must be assigned a unique filter precedence.
Start Network	Specify the first IPX network number in the range.
End Network	Specify the last IPX network number in the range.
Direction	Select the direction of the filter from a pull-down menu. The pull-down filter menu options are: • **Inbound** - Apply the filter only to RIP packets received on the interface. • **Outbound** - Apply the filter only to RIP packets sent on the interface. • **Both** - Apply the filter to RIP packets both sent and received on the interface.

Table 13-2. Add IPX RIP Filters Dialog Box Parameters continued

Parameter	Allows you to...
Filter/Suppress	Disable the IPX networks (within the specified range in the filter) to be filtered (inbound) or suppressed (outbound). • **Filtered** - Apply the filter only to RIP packets received (inbound direction) on the interface. • **Suppressed** - Apply the filter only to RIP packets sent (outbound direction) on the interface. **Enable** allows you to filter and suppress traffic and is the default. Select **Disable** to disable the filtering and suppression of traffic.
Ticks	Specify the time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second. This entry is used to override the value in the RIP packet. If you enter **0**, there will be no override in the transmission of data on the network.
Hops	Specify the number of routers (hops) that the packet must pass through before reaching the network number associated with the IPX interface. This entry is used to override the value in the RIP packet. If you enter **0**, there will be no override in the transmission of data on the network.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Example #1: Configuring your switch to suppress advertising of network 10

To configure your switch to suppress the advertising of network 10 on the IPX interface named Backbone, complete the following steps:

1. Select Filters from the Routing > IPX > RIP group in the Web Agent window. The IPX RIP Filters dialog box opens (Figure 13-2).
2. Select Create to create a new filter. The Add IPX RIP Filter dialog box opens (Figure 13-3).

3. Configure the following parameters on the Add IPX RIP Filter dialog box:

   a. Select Backbone from the Interface pull-down menu.

   b. Enter 0 in the Precedence field.

   c. Enter 10 in the Start Network field.

   d. Enter 10 in the End Network field.

   e. Open the Direction pull-down menu and select Outbound.

   f. Open the Filter/Suppress pull-down menu and select Enable.

   g. Enter 0 in the Ticks and Hops fields.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

The filter created in this example ensures that all advertising of network 10 from the interface labeled Backbone is suppressed.

Example #2: Suppress Advertising of all Networks Except 10

To configure your switch to suppress the advertising of all networks except network 10 on the IPX interface named Backbone, you must first create two filters.

To create filter 1 from the web agent:

1. Select Filters in the Routing > IPX > RIP group on the web agent window. The IPX RIP Filter dialog box opens (see Figure 13-2).
2. Select Create to create a new filter. The Add IPX RIP Filter dialog box opens.
3. Configure the following parameters:

   a. Select Backbone from the Interface pull-down menu.

   b. Enter 0 in the Precedence field.

   c. Enter 10 in the Start Network field.

   d. Enter 10 in the End Network field.

   e. Select Outbound from the Direction pull-down menu.

   f. Select Disable from the Filter/Suppress pull-down menu.

g. Enter 0 in the Ticks and Hops fields.

Filter 1 ensures that the advertising of network 10 on the interface Backbone will not be suppressed. To suppress all other networks, proceed with the creation of Filter 2.

To create Filter 2 from the web agent:

1. Repeat steps 1- 2 in the creating Filter #1 procedure.
2. Configure the following parameters:
   - **a.** Select Backbone from the Interface pull-down menu.
   - **b.** Enter 1 in the Precedence field.
   - **c.** Enter 0 in the Start Network field.
   - **d.** Enter ffffffff in the End Network field.
   - **e.** Select Outbound from the Direction pull-down menu.
   - **f.** Select Enable from the Filter/Suppress pull-down menu.
   - **g.** In the Ticks and Hops fields, enter 0, respectively.
3. Click CREATE to save your changes, or CANCEL to restore previous settings.

Filter 2 ensures that the advertising of all networks on the interface Backbone will be suppressed.

Together, Filter 1 and Filter 2 will act to suppress all network advertising with the *exception* of *network 10*. It is important to note that Filter 2 had the Precedence field set to **1** and Filter 1 had the Precedence field set to **0**. Any filter with a Precedence of 0 will always override a filter with a precedence of 1 or higher.

Creating and Modifying IPX RIP Filters Using the CLI

To create and modify IPX RIP filters using the CLI, enter the following command from Priv mode:

```
cajun# ipx rip-filter <precedence> <start-network>
<end-network> {outbound|inbound|both} {filter|
allow} [<filter-ticks> [<filter-hops>]]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

14 Configuring IPX SAP Protocol

Overview

The information and procedures provided in this chapter pertain to layer 3 module configuration only. This chapter provides the following procedures:

- Configuring Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) Interfaces
- Creating IPX SAP Filters
- Interpreting IPX SAP Interface Statistics

Configuring Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) Interfaces

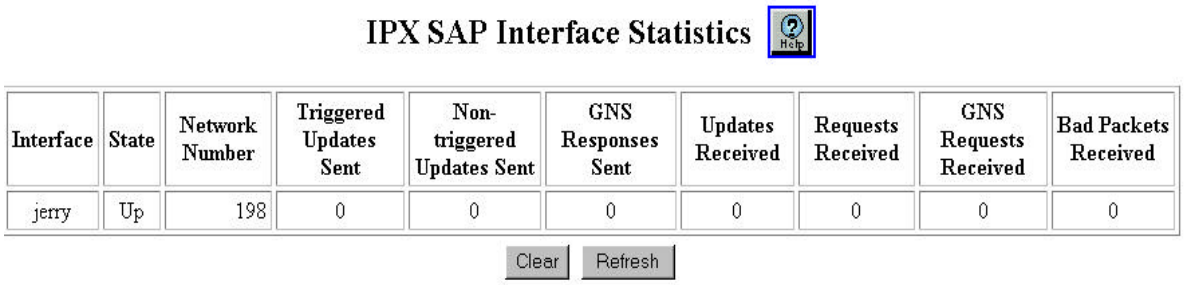
You can configure IPX SAP using either the web agent or the CLI.

Configuring IPX SAP Interfaces Using the Web Agent

To configure the IPX SAP interfaces using the web agent:

1. Select Interfaces from the Routing > IPX > SAP group on the Web Agent window. The IPX SAP Interfaces dialog box opens (Figure 14-1).

Figure 14-1. IPX SAP Interfaces Dialog Box



2. Refer to Table 14-1 to configure the IPX SAP Interface dialog box parameters:

Table 14-1. IPX SAP Interface Dialog Box Parameters

Parameter	Allows you to...
Select	Select a SAP interface to modify.
Interface	Identifies the IPX interface associated with the SAP interface.
Network Number	Identifies the number of the IPX network associated with the interface.
Use Interpacket Gap	Select one of the following from the pull-down menu: • **Disable –** if you do not want the IPX SAP periodic update packets to be sent out over an interface with no interpacket transmission delay. • **Enable** – If you want to send the IPX SAP periodic update packets to be sent out over an interface with an interpacket transmission delay (default).
Use Max Packet Size	Select one of the following from the pull-down menu: • **Disable –** To limit SAP packets to 7 service entries • **Enable** – To allow SAP) packets to contain the maximum number of services entries that are allowed by the SAP Interface MTU (default).
Periodic Update Interval (sec)	Enter (in seconds) the interval at which periodic SAP updates are sent out an interface.
Aging Interval Multiplier	Enter the length of time that information from received SAP updates are kept as a multiplier of the Periodic Update Interval.

Table 14-1. IPX SAP Interface Dialog Box Parameters continued

Parameter	Allows you to...
Triggered Updates	Select one of the following from the pull-down menu: • **Disable –** To prevent SAP updates from being immediately transmitted to the network in response to changes in the network topology • **Enable** – To allow SAP updates to be immediately transmitted to the network in response to changes in the network topology (default).
Get Nearest Server Reply	Select one of the following from the pull-down menu: • **Disable –** To prevent the router from responding to **Get Nearest Server** requests received on the interface • **Enable** – To allow the router to respond to **Get Nearest Server** requests received on the interface (default).
Get Nearest Server Reply Delay	Specify the delay (in msecs) to wait before responding to a Get Nearest Service request received on the interface.
Mode	Select one of the following from the pull-down menu: • **Talk/Listen** - Send and receive advertisements (default). • **Talk Only** - Send advertisements. • **Listen Only** - Receive advertisements.

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring IPX SAP Interfaces Using the CLI

To configure the IPX SAP interfaces using the CLI, enter the following command from Interface mode:

```
cajun(conf-if <interface-name>):# ipx sap
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating IPX SAP Filters

This section provides the following procedures:

- Creating IPX SAP Name Filters
- Creating IPX SAP Network Filters

Creating IPX SAP Name Filters

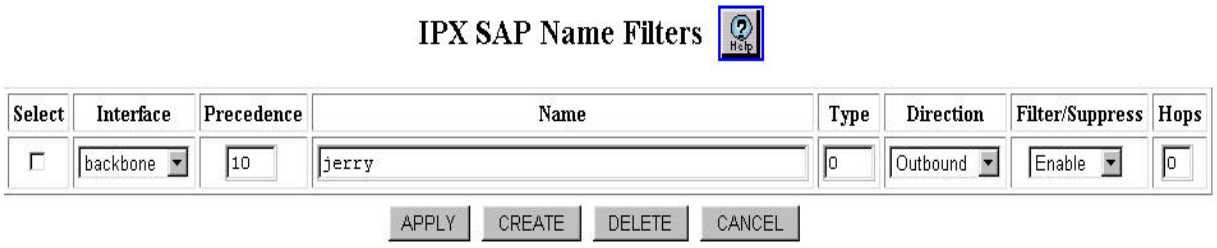
You can create IPX SAP name filter suing either the web agent or the CLI.

Creating IPX SAP Name Filters Using the Web Agent

To create IPX SAP name filters using the web agent:

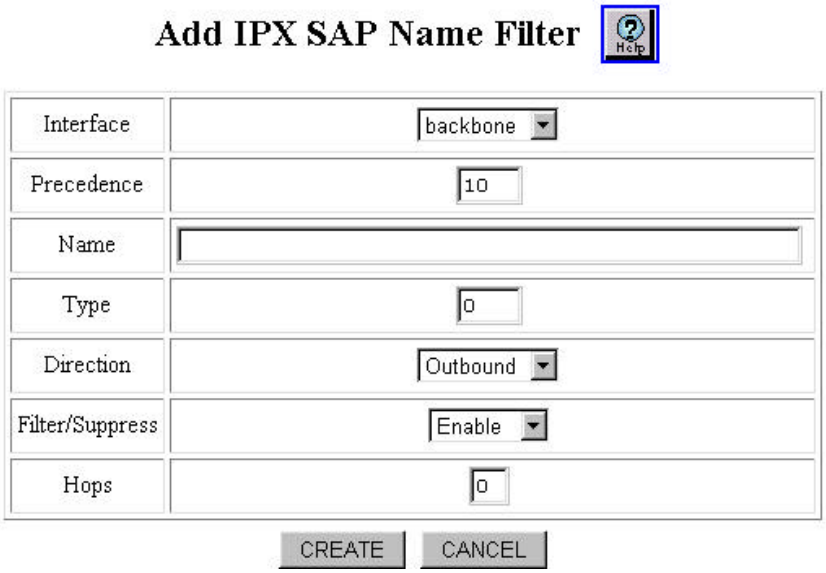
1. Select Name Filters from the Routing > IPX > SAP group on the Web Agent window. The IPX SAP Name Filters dialog box opens (Figure 14-2).

Figure 14-2. IPX SAP Name Filters Dialog Box.



2. Select CREATE to create a new filter. The Add IPX SAP Name Filter dialog box opens (Figure 14-3).

Figure 14-3. Add IPX SAP Name Filter Dialog Box



3. Configure an IPX SAP name filter. Refer to Table 14-2 for an explanation of the Add IPX SAP Name Filter dialog box parameters:

Table 14-2. IPX SAP Name Filter Dialog Box Parameters

Parameter	Allows you to...
Interface	Select the interface to which this filter will be applied to SAP packets sent and/or received on the interface from the pull-down menu.
Precedence	Enter the filter precedence (in order of importance) with 0 equal to most important. **Note:** All SAP filters on the same interface must be assigned a unique precedence value.
Name	Enter a service name. For example, FS_ENG001. A single asterisk may be present as the last character, which will match all remaining characters of a service name.

Table 14-2. IPX SAP Name Filter Dialog Box Parameters continued

Parameter	Allows you to...
Type	Enter the service type that identifies the type of service the server provides. Well-known service types include: • Unknown (0) • Print Queue (3) • File Server (4) • Job Server (5) • Print Server (7) • Archive Server (9) • Remote Bridge Server (24) • Advertising Print Server (47) • NetWare Directory Services [NDS] (278) A value of ffff matches all service type values.
Direction	Select the filter direction from the following pull-down menu options: • **Inbound** - Applies the filter only to SAP packets received on the interface. • **Outbound** - Applies the filter only to SAP packets sent on the interface. • **Both** - Applies the filter to SAP packets both sent and received on the interface.
Filter/Suppress	Select to enable or disable whether the services matching Name and Type are filtered (inbound) or suppressed (outbound). • **Filtered** - Applies the filter only to SAP packets received (inbound direction) on the interface. • **Suppressed** - Applies the filter only to SAP packets sent (outbound direction) on the interface. Select **Enable** to filter/suppress traffic. Select **Disable** to disable the filtering and suppression of traffic.
Hops	Specify the number of routers (hops) that the packet must pass through before reaching the service(s) matched by the filter. This entry is used to override the value in the SAP packet. Entering 0 ensures that there is no override in the transmission of data on the network.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Example: Suppress Advertising of all Print Servers on Interface Remote

To configure your switch to suppress the advertising of all Print Servers (for example, type 7) on Interface Remote:

1. Select Name Filters from the Routing > IPX > SAP group on the web agent window. The IPX SAP Name Filters dialog box opens (Figure 14-2).
2. Click CREATE to create a new filter. The Add IPX SAP Name Filter dialog box opens (Figure 14-3).
3. Configure the following parameters:
   a. Select Remote from the Interface pull-down menu.
   b. Enter 0 in the Precedence field.
   c. Enter * (asterisk) in the Name field. The asterisk represents a wildcard that applies to all server names.
   d. Enter 7 in the Type field.
   e. Select Outbound from the Direction pull-down menu.
   f. Select Enable from the Filter/Suppress pull-down menu.
   g. Enter 0 in the Hops field. This ensures that there is no override in the transmission of data on the network.
4. Click CREATE to save your changes, or CANCEL to restore previous settings.

*** Note:** This filter ensures that all advertising of any known print server on Interface Remote will be suppressed.

Creating IPX SAP Name Filters Using the CLI

To create IPX SAP name filters using the CLI, enter the following command from Priv mode:

```
cajun# ipx sap-name-filter <precedence>
<filter-name> <service-type>
{outbound|inbound|both} {filter| allow}
[<filter-hops>]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating IPX SAP Network Filters

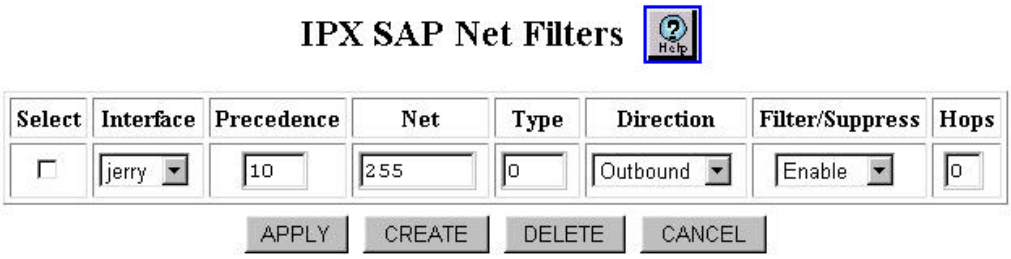
You can create IPX SAP network filters using wither the web agent or the CLI.

Creating IPX SAP Network Filters Using the Web Agent

To create IPX SAP Network filters using the web agent:

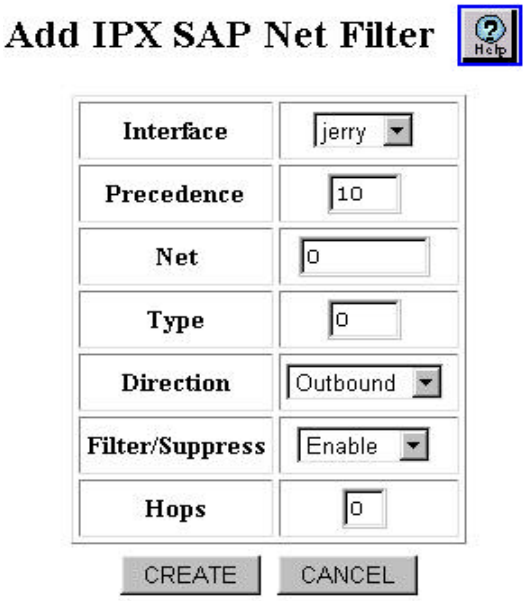
1. Select Net Filters from the Routing > IPX > SAP group on the Web Agent window. The IPX SAP Net Filters dialog box opens (Figure 14-4).

Figure 14-4. IPX SAP Net Filters Dialog Box



2. Select CREATE. The Add IPX SAP Net Filter dialog box opens (Figure 14-5).

Figure 14-5. Add IPX SAP Net Filter Dialog Box



3. Refer to Table 14-3 to configure the Add IPX SAP Net Filters dialog box parameters:

Table 14-3. Add IPX SAP Network Filter Dialog Box Parameters

Parameter	Allows you to...
Select	Select the IPX interface. **Note:** This field is displayed in the **IPX SAP Net Filter** dialog box, not in the **Add IPX SAP Net Filter** dialog box.
Interface	Select the interface to which this filter will be applied to SAP packets sent and/or received on the interface.
Precedence	Specify the filter precedence (in order of importance) with 0 equal to most important. **Note:** All SAP filters on the same interface must be assigned a unique filter precedence.
Net	Specify the network on which the server resides. A network number of ffffffff represents all networks.
Type	Specify the service type (in hex) that identifies the type of service the server provides. Well-known service types include: • Unknown (0) • Print Queue (3) • File Server (4) • Job Server (5) • Print Server (7) • Archive Server (9) • Remote Bridge Server (24) • Advertising Print Server (47) • NetWare Directory Services (278) A value of ffff matches all service type values.
Direction	Select the direction of the filter in question. Filter choices include: • **Inbound** - Applies the filter only to SAP packets received on the interface. • **Outbound** - Applies the filter only to SAP packets sent on the interface. • **Both** - Applies the filter to SAP packets both sent and received on the interface

Table 14-3. Add IPX SAP Network Filter Dialog Box Parameters
continued

Parameter	Allows you to...
Filter/ Suppress	Disable whether the services matching Net and Type are filtered (inbound) or suppressed (outbound). • **Filtered** - Applies the filter only to SAP packets received (inbound direction) on the interface. • **Suppressed** - Applies the filter only to SAP packets sent (outbound direction) on the interface. Select **Disable** to disable the filtering and suppression of traffic. The default is **Enable**.
Hops	Specify the number of routers (hops) that the packet must pass through before reaching the service(s) matched by the filter. This entry is used to override the value in the SAP packet. Entering 0 ensures that there is no override in the transmission of data on the network.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Example: Filtering all Services Except Netware Directory Services (NDS)

To configure your switch to filter all services except NDS a specific Interface, you must create two filters. Together, Filter 1 and Filter 2 filter services learned on the indicated interface except for NDS advertisements.

To create these filters using the web agent:

Filter 1

This filter ensures that all NDS packets received are not filtered on Interface Remote.

1. Select Net Filters from the Routing > IPX > SAP group on the Web Agent window. The IPX SAP Net Filters dialog box opens (Figure 14-4).
2. Click CREATE to create a new filter. The Add IPX SAP Net Filter dialog box opens (Figure 14-5).

3. Configure the following parameters:

   a. Select an interface name from the Interface pull-down menu.

   b. Enter 0 in the Precedence field.

      * **Note:** Any filter with a Precedence of 0 will always override a filter with a precedence of 1 or higher.

   c. Enter ffffffff (which represents all networks) in the Net field.

   d. Enter 278 (which represents the type for NDS) in the Type field.

   e. Select Inbound from the Direction pull-down menu.

   f. Select Disable from the Filter/Suppress pull-down menu to ensure that NDS advertisements are not filtered.

   g. Enter 0 in the Hops field to ensure that there is no override in the transmission of data on the network.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Filter 2

Filter 2 ensures that all networks and service types are filtered for the indicated interface.

1. Select Net Filters from the Routing > IPX > SAP group on the Web Agent window. The IPX SAP Net Filters dialog box opens (Figure 14-4).

2. Click CREATE to create a new filter. The Add IPX SAP Net Filter dialog box opens (Figure 14-5).

3. Configure the following parameters:

   a. Select an interface name from the Interface pull-down menu.

   b. Enter 1 in the Precedence field.

   c. Enter ffffffff (which represents all networks) in the Net field.

   d. Enter ffff (which represents all services/types) in the Type field.

e. Select Inbound from the Direction pull-down menu.

f. Select Enable from the Filter/Suppress pull-down menu.

g. Enter 0 in the Hops field. Entering 0 ensures that there is no override in the transmission of data on the network.

4. Click CREATE to save your changes, or CANCEL to restore previous settings.

Creating IPX SAP Network Filters Using the CLI

To create IPX SAP Network filters using the CLI, enter the following command from Interface mode:

```
cajun(config if-<interface name>)# ipx
sap-network-filter <precedence> <filter-network>
<service-type> {outbound|inbound | both}
{filter|allow} [<filter-hops>]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Interpreting IPX SAP Interface Statistics

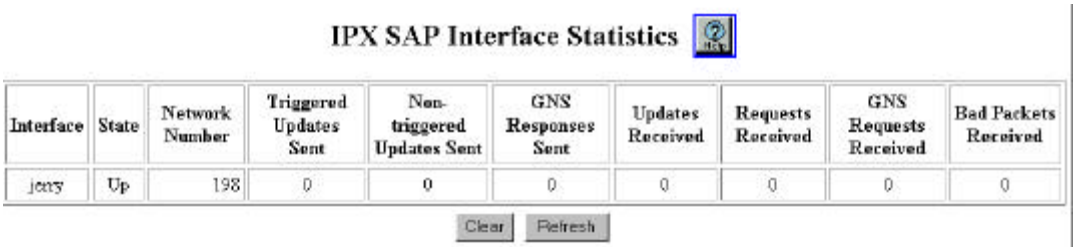
You can interpret IPX SAP interface statistics using either the web agent or the CLI.

Interpreting IPX SAP Interface Statistics Using the Web Agent

To interpret IPX SAP interface statistic using the web agent:

1. Select Interface Statistics from the Routing > IPX > SAP group on the Web Agent window. The IPX SAP Interface Statistics dialog box opens (Figure 14-6).

Figure 14-6. IPX SAP Interface Statistics Dialog Box



2. Refer to Table 14-4 to interpret your IPX SAP interface statistics:

Table 14-4. IPX SAP Interface Statistical Parameters

Parameter	Definition
Interface	The IPX interface associated with this SAP interface.
State	The current state of the SAP interface.
Network Number	The network number of the IPX network associated with the interface.
Triggered Updates Sent	The number of triggered updates sent from the SAP interface.
Non-triggered Updates Sent	The number of non-triggered updates sent from the SAP interface.
GNS Responses Sent	The number of GNS responses sent from the SAP interface.
Updates Received	The number of updates received. Updates may be received periodically even if no changes have occurred.
Requests Received	The number of requests received on the SAP interface.
GNS Requests Received	The number of GNS requests received on the SAP interface.
Bad Packets Received	The number of bad packets received on the SAP interface.

3. Click on CLEAR to remove the statistics, or REFRESH to access current interface statistics.

Interpreting IPX SAP Interface Statistics Using the CLI

To interpret IPX SAP interface statistics using the CLI, enter the following command from Interface mode:

```
cajun(config-if <interface name>)# show ipx
interface [<intf-name>]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

15 Configuring AppleTalk Routing

Overview

The following information and procedures provided in this chapter pertain to layer 3 module configuration only:

- AppleTalk Routing Overview
- Configuring AppleTalk Routing
- Viewing AppleTalk Statistics

AppleTalk Routing Overview

AppleTalk Phase I was originally designed for local work groups. AppleTalk Phase II extends the number of nodes in an internetwork to over 16 million and the number of zones per port to 254. The Cajun switch supports both AppleTalk Phase I and Phase II. However, the translation from AppleTalk Phase I to Phase II is not supported.

The Cajun P550/P880/P882 switch software, version 5.0, supports AppleTalk routing for packets destined across VLANs (inter-VLAN) using layer 3 but for intra-VLAN traffic, layer 2 switching is supported.

*** Note:** The Cajun P550/P880/P882 switch supports AppleTalk over Ethernet only.

Ethernet versions supported:

- Ethernet SNAP
- Ethernet II

The Cajun P550/P880/P882 switch supports the following AppleTalk protocols:

- AppleTalk Address Resolution Protocol (AARP)
- Routing Table Maintenance Protocol (RTMP)
- Name-Binding Protocol (NBP)
- AppleTalk Echo Protocol (AEP)
- Datagram Delivery Protocol (DDP)
- Zone Information Protocol (ZIP)

Configuring AppleTalk Routing

This section includes:

- Enabling AppleTalk Global Routing
- Creating an AppleTalk Routing Interface
- Editing AppleTalk Interfaces
- Deleting an AppleTalk Interface
- Creating an AppleTalk Static Route
- Editing AppleTalk Static Routes
- Deleting an AppleTalk Static Route
- Creating an AppleTalk Name-Binding Protocol (NBP) Filter
- Editing an AppleTalk NBP Filter
- Adding or Deleting Interfaces to an NBP Filter
- Creating an AppleTalk Zone Filter
- Editing an AppleTalk Zone Filter
- Adding or Deleting Interfaces to a Zone Filter

Enabling AppleTalk Global Routing

To enable AppleTalk routing globally:

1. Select **Global Configuration** from the **Routing>Appletalk>Configuration** group on the web agent window. The **AppleTalk Routing Global Configuration** dialog box opens (Figure 15-1).

Figure 15-1. AppleTalk Routing Global Configuration Window

2. Select **Enable** from the **AppleTalk Routing** pull-down menu.

3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

Creating an AppleTalk Routing Interface

You can create an AppleTalk routing interface using the web agent or CLI.

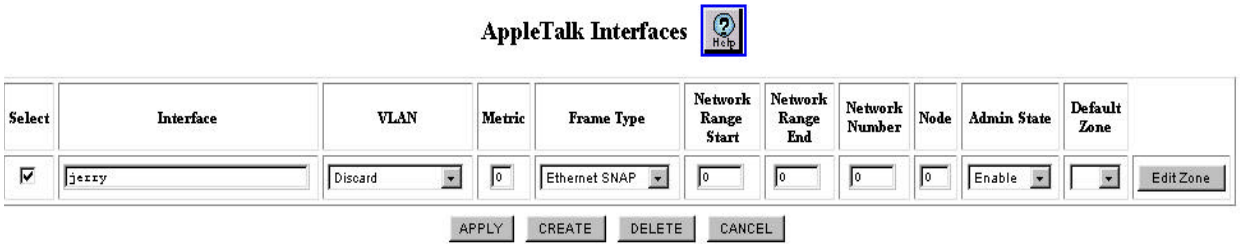
Creating an AppleTalk Routing Interface Using the Web Agent

To create an AppleTalk routing interface using the web agent:

1. Enable AppleTalk routing globally. Refer to "Enabling AppleTalk Global Routing"", earlier in this chapter.

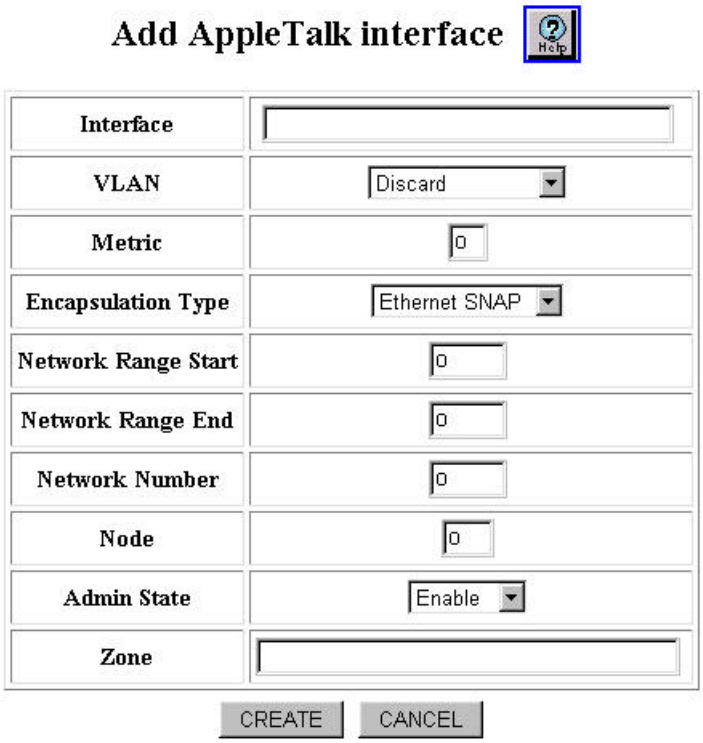
2. Select **Interfaces** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box opens (Figure 15-2).

Figure 15-2. AppleTalk Interfaces Dialog Box



3. Select **CREATE**. The **Add AppleTalk Interfaces** dialog box opens (Figure 15-3).

Figure 15-3. Add AppleTalk Interfaces Dialog Box



4. Refer to Table 15-1 to configure the **Add AppleTalk Interface** dialog box parameters:

Table 15-1. Add AppleTalk Interface Dialog Box Parameters

Parameter	Definition
Interface	Enter the name of the AppleTalk interface to be created.
VLAN	Select the VLAN to be associated with the AppleTalk interface. The options include: • Default • Discard • All created VLANs
Metric	Enter the metric associated with the AppleTalk interface.
Encapsulation Type	Select the encapsulation type to be associated with the AppleTalk interface.The options include: • **Ethernet II** - MTU = 1500 • **Ethernet SNAP** - MTU =1492

Table 15-1. Add AppleTalk Interface Dialog Box Parameters
continued

Parameter	Definition
Network Range Start	Enter the starting network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 0 and 65279. **Note:** The Network Range Start value must be less than or equal to the Network Range End value.
Network Range End	Enter the ending network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 0 and 65279. **Note:** If the Network Range Start value equals 0, then the Network Range End value must also equal 0.
Network Number	Enter the interface network number. This number specifies the network number the interface is using. **Note:** This value must be within the Network Range or be equal to 0.
Node	Enter the interface node identification number. This number must be between 1 and 253. **Note:** Only if the Network Number is equal to 0, can the Node also be equal to 0.
Admin State	Select whether to enable or disable the administrator state. The administrator state determines if the interface is operational from a management point of view.
Zone	Select the default AppleTalk zone to be used by this interface. Zone names may be up to 32 characters in length.

5. Click **CREATE** to add the new AppleTalk interface, or **CANCEL** to restore previous settings.

Creating an AppleTalk Routing Interface Using the CLI

To create an AppleTalk interface using the CLI. enter the following command in **Configure** mode:

```
> (config if-:<interface-name>)# appletalk routing
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Editing AppleTalk Interfaces

You can edit AppleTalk interfaces using either the web agent or the CLI.

Editing AppleTalk Interfaces Using the Web Agent

To edit an AppleTalk interface using the web agent:

*** Note:** You must enable AppleTalk globally and create an AppleTalk interface before you can edit an interface. See "Enabling AppleTalk Global Routing" and "Creating an AppleTalk Routing Interface", earlier in this section.

1. Select **Interfaces** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box opens (Figure 15-2).
2. Select the **VLAN** to be associated with the interface from the **VLAN** field pull-down menu.
3. Enter the **new port metric** to be associated with the interface in the **Metric** field.
4. Select the **new frame type** to be associated with the interface from the **Frame Type** pull-down menu.
5. Enter the **new network range start number** in the **Network Range Start** field.
6. Enter the **new network range end number** in the **Network Range End** field.
7. Enter the **new network number** to be associated with the interface in the **Network Number** field.
8. Enter the **new node number** to be associated with the interface in the **Node** field.
9. Select **Enable** from the **Admin. State** field pull-down menu.
10. Select the **new default zone** associated with the interface from the **Default Zone** field pull-down menu.

*** Note:** If there is no zone to select or if you want to edit the zones available, complete steps 11 through 14. Otherwise, proceed to step 15.

11. Select **Edit Zone** to edit the AppleTalk zone for this interface. The **Edit AppleTalk Zone** dialog box opens (Figure 15-4).

Figure 15-4. Edit AppleTalk Zone Dialog Box

12. Enter the new AppleTalk zone in the **Add** text field and click **Add**.

13. Click **Apply** to save the new AppleTalk zone, or either **Delete** or **Cancel** to remove the new zone.

14. Select **Interfaces** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box re-opens (Figure 15-2)

15. Select the new zone that you just created from the **Default Zone** field pull-down menu.

16. Select the check box for the AppleTalk interface that you want to update in the **Select** column.

17. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

*** Note:** You may select and change as many interfaces simultaneously with one APPLY operation.

Editing AppleTalk Interfaces Using the CLI

To edit an AppleTalk interface using the CLI, enter the following command from **Configure** mode:

```
> (config if-:<interface-name>)# appletalk <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting an AppleTalk Interface

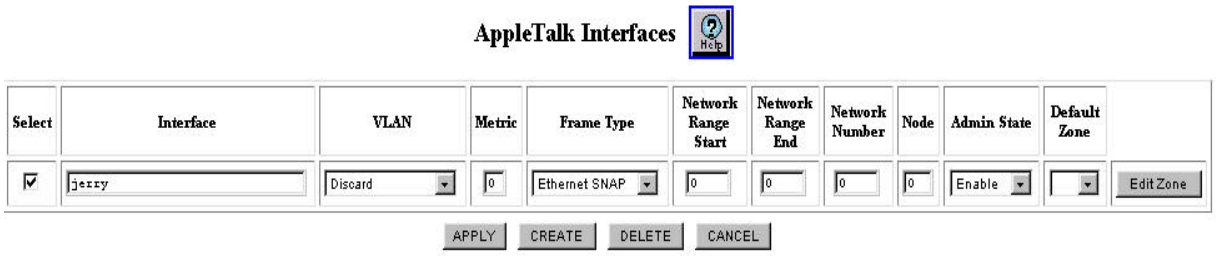
You can delete an AppleTalk interface using either the web agent or the CLI.

Deleting an AppleTalk Interface Using the Web Agent

To delete an AppleTalk interface using the web agent:

1. Select **Interfaces** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box opens (Figure 15-5).

Figure 15-5. AppleTalk Interfaces Dialog Box



2. Select the checkbox for the **AppleTalk interface** that you want to delete from the **Select** column.

3. Click **DELETE** to remove the AppleTalk interface.

Deleting an AppleTalk Interface Using the CLI

To delete an AppleTalk interface using the CLI, enter the following command from **Configure** mode:

```
> (config if-<interface-name>:)# no appletalk
routing
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating an AppleTalk Static Route

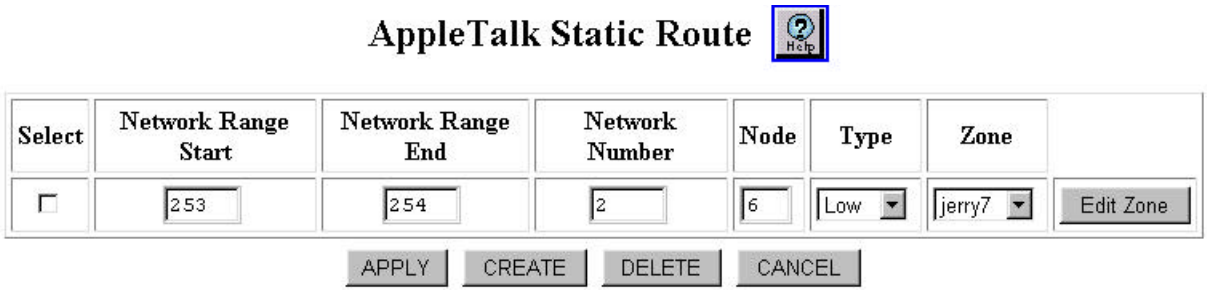
You can create an AppleTalk static route using the web agent or the CLI.

Creating an AppleTalk Static Route Using the Web Agent

To create an AppleTalk static route using the web agent:

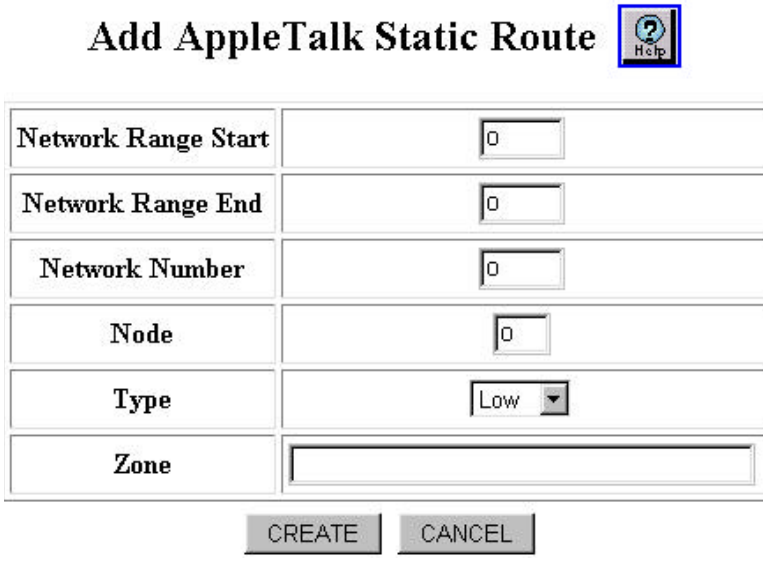
1. Select **Static Route** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk Static Route** dialog box opens (Figure 15-6).

Figure 15-6. AppleTalk Static Route Dialog Box



2. Select **CREATE** to add a new static route. The **Add AppleTalk Static Route** dialog box opens (Figure 15-7).

Figure 15-7. Add AppleTalk Static Route Dialog Box



3. Refer to Table 15-2 to configure the **Add AppleTalk Static Route** dialog box parameters.

Table 15-2. Add AppleTalk Static Route Dialog Box Parameters

Parameter	Definition
Network Range Start	Enter the starting network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 1 and 65279. **Note:** Network Range Start must be less than or equal to Network Range End.
Network Range End	Enter the ending network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 1 and 65279.
Network Number	Enter the next hop network number. This number specifies the network number of the next hop router for the network range.
Node	Enter the next hop node identification number. This number must be between 1 and 253.
Type	Select the type of static route. The options include: • **High** - The static route is not superseded by a route update. • **Low** - The static route can be superseded by a route update.
Zone	Enter an AppleTalk zone name assigned to this route. Zone names may be up to 32 characters in length.

4. Click **CREATE** to add the static route, or **CANCEL** to restore previous settings.

Creating an AppleTalk Static Route Using the CLI

To create an AppleTalk static route using the CLI, enter the following command in **Configure** mode:

```
> (config if-<interface-name>:)# appletalk
static cable-range <cable-range> to <network.node>
[floating] zone <zone-name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Editing AppleTalk Static Routes

You can edit AppleTalk Static routes using either the web agent or the CLI.

Editing AppleTalk Static Routes Using the Web Agent

To edit an AppleTalk static route using the web agent:

1. Select **Static Route** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk Static Route** dialog box opens (Figure 15-6).
2. Select the checkbox next to the **AppleTalk Static Route** that you want to edit from the **Select** column.
3. Enter the **new network range start number** in the **Network Range Start** field.
4. Enter the **new network range end number** in the **Network Range End** field.
5. Enter the **new network number** of the next hop for the static route in the **Network Number** field.
6. Enter the **new node number** of the next hop for the static route in the **Node** field.
7. Enter the type to be associated with the static route in the **Type** field.
8. Select **Edit Zone**. The **Edit AppleTalk Zone** dialog box opens (see Figure 15-4).
9. Enter the **new AppleTalk** z**one network range** and click **Add** in the **Add** text field.
10. Click **APPLY** to save the new zone, or **Delete** or **CANCEL** to ignore the new zone.

Editing AppleTalk Static Routes Using the CLI

To edit an AppleTalk static route using the CLI, enter the following command from **Configure** mode:

```
> (config if-:<interface-name>)# appletalk
static cable-range <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting an AppleTalk Static Route

You can delete an AppleTalk static route using either the web agent or the CLI.

Deleting an AppleTalk Static Route Using the Web Agent

To delete an AppleTalk static route using the web agent:

1. Select **Static Route** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk Interfaces** dialog box opens (Figure 15-5).
2. Select the checkbox next to the AppleTalk static route that you want to delete from the **Select** column.
3. Click **DELETE** to remove the AppleTalk static route.

Deleting an AppleTalk Static Route Using the CLI

To delete an AppleTalk static route using the CLI, enter the following command in **Configure** mode:

```
> (config if-<interface-name>:)# no appletalk
static
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating an AppleTalk Name-Binding Protocol (NBP) Filter

The NBP performs a conversion from named AppleTalk entities to their AppleTalk protocol addresses. Multiple names can exist for the same entity (alias). NBP also performs:

- Name registration
- Name deletion
- Name lookup
- Name confirmation

NBP allows you to bind a name to the internal storage address for your entity and register this mapping so that other entities can look it up. You can display NBP names to users and use addresses internally to locate entities. When you register your entity's name and address pair, NBP validates its uniqueness.

You can create an NBP using either the web agent or the CLI.

Creating a NBP Filter Using the Web Agent

To create an NBP filter using the web agent:

1. Select **NBP Filter** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk NBP Filter** dialog box opens (Figure 15-8).

Figure 15-8. AppleTalk NBP Filter Dialog Box

2. Select **CREATE** to add a new NBP filter. The **Add AppleTalk NBP Filter** dialog box opens (Figure 15-9).

Figure 15-9. Add AppleTalk NBP Filter Dialog Box

3. Refer to Table 15-3 to configure the **Add AppleTalk NBP filter** dialog box.

Table 15-3. AppleTalk NBP Filter Parameters

Parameter	Definition
Access List	Enter the access list number to be associated with the NBP filter. Valid values are 600-631.
Name	Enter the name of the NBP name object to be filtered.
Type	Select the type of filtering. The options include: • **Deny** • Permit **Note:** You can also leave this field blank for wildcarding:
Interface	Select the interface(s) to apply this filter to.

4. Click **CREATE** to add your new static route, or **CANCEL** to restore previous settings.

Creating a NBP Filter Using the CLI

To create an NBP filter using the CLI, enter the following command from **Configure** mode:

```
> (config-if <interface-name>:)# appletalk
access-list <access-list-number>
<permit|deny> nbp <string>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Editing an AppleTalk NBP Filter

You can edit an AppleTalk NBP filter using either the web agent or the CLI.

Editing an AppleTalk NBP Filter Using the Web Agent

To edit an AppleTalk NBP filter using the web agent:

1. Select **NBP Filter** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk NBP Filter** dialog box opens (Figure 15-8).
2. Refer to Table 15-3 to edit the **AppleTalk NBP Filter** dialog box parameters.
3. Click ...
   - **CREATE** to add a new filter. The Add AppleTalk NBP Filter dialog box opens. See "Creating an AppleTalk NBP Filter", earlier in this section, for more information.
   - **DELETE** to remove the selected NBP filter.
   - **CANCEL** to restore previous settings.
   - **Edit If** to add or delete this NBP filter to/from an interface. The Add/Delete Interface to NBP Filter dialog box opens. See "Adding or Deleting Interfaces to NBP Filter", later in this section, for more information.

Editing an AppleTalk NBP Filter Using the CLI

To edit an AppleTalk NBP filter using the CLI, enter the following command in **Configure** mode:

```
> (config-if <interface-name>:)# appletalk
access-list <access-list-number>
<permit|deny> nbp <string>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Adding or Deleting Interfaces to an NBP Filter

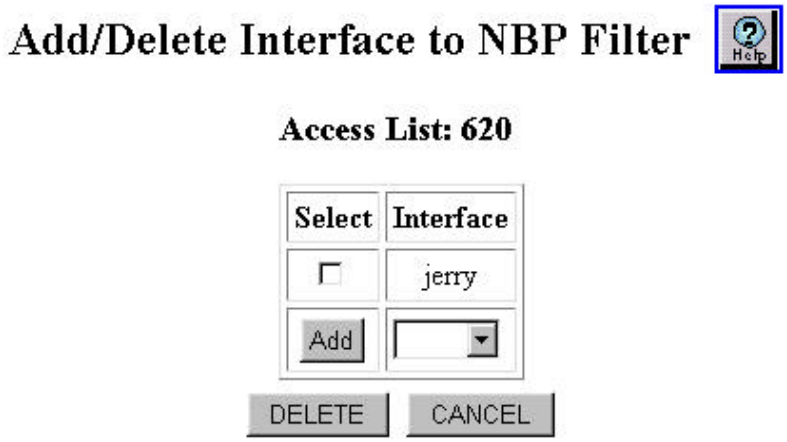
You can add or delete interfaces to an NBP filter using either the web agent or the CLI.

Adding or Deleting Interfaces to an NBP Filter Using the Web Agent

To add or delete interfaces to an NBP filter using the web agent:

1. Select **NBP Filter** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk NBP Filter** dialog box opens (see Figure 15-8).
2. Select **Edit If**. The **Add/Delete Interface to NBP Filter** dialog box opens (see Figure 15-10).

Figure 15-10. Add/Delete Interface to NBP Filter Dialog Box



3. Select the interface to be added from the **Add** field pull-down menu.

   Or

   Click the checkbox in the **Select** column for the interface that you want to be remove.

4. Click ...

   — **Add** to add this NBP filter to the selected interface.

   — **DELETE** to remove this NBP filter from the selected interface.

   — **CANCEL** to restore previous settings.

Adding or Deleting Interfaces to NBP Filter Using the CLI

To add interfaces to an NBP filter using the CLI, enter the following command from **Configure** mode:

```
> (config-if <interface-name>:)# appletalk
access-list <access-list-number>
<permit|deny> nbp <string>
```

To delete interfaces to an NBP filter using the CLI, enter the following command from **Configure** mode:

```
> (config-if <interface-name>:)# no appletalk
access-list <access-list-number>
<permit|deny> nbp <string>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Creating an AppleTalk Zone Filter

You can create an AppleTalk Zone Filter using either the web agent or the CLI.

Creating an AppleTalk Zone Filter Using the Web Agent

To create an AppleTalk zone filter using the web agent:

1. Select **Zone Filter** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk Zone Filter** dialog box opens (Figure 15-11).

Figure 15-11. AppleTalk Zone Filter Dialog Box

2. Select **CREATE**. The **Add AppleTalk Zone Filter** dialog box opens (see Figure 15-12).

Figure 15-12. Add AppleTalk Zone Filter Dialog Box

3. Refer to Table 15-4 to configure the **Add AppleTalk Zone Filter** dialog box parameters:

Table 15-4. Add AppleTalk Zone Filter Dialog Box Parameters

Parameter	Definition
Access List	Enter the access list number to be associated with the zone filter. Valid values are 632-663.
Name	Enter the name of the zone to be filtered. You can also leave this field blank for wildcarding.
Type	Select the type of filtering. The options include: • **Deny** • **Permit**
Interface	Select the interface to apply this filter to.

4. Click **CREATE** to add the new zone filter, or **CANCEL** to restore previous settings.

Creating an AppleTalk Zone Filter Using the CLI

To create an AppleTalk zone filter using the CLI, enter the following command from **Configure** mode:

```
>(config-if <interface-name>:)# appletalk access-list <access-list-number> <permit|deny> zone <string>
```

Refer to the *Cajun™ P550™/P880/P882 CP880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Editing an AppleTalk Zone Filter

You can edit an AppleTalk zone filter using either the web agent or the CLI.

Editing an AppleTalk Zone Filter Using the Web Agent

To edit an AppleTalk zone filter using the web agent:

1. Select **Zone Filter** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk Zone Filter** dialog box opens (Figure 15-12).
2. Click the checkbox in the **Select** column next to the AppleTalk zone filter that you want to be edit.
3. Refer to Table 15-4 to edit the **AppleTalk Zone Filter** dialog box parameters:.
4. Click ...
   - **CREATE** to add a new zone filter. The **Add AppleTalk Zone Filter** dialog box opens. See "Creating an AppleTalk Zone Filter", earlier in this section for more information.
   - **DELETE** to remove the selected zone filter.
   - **CANCEL** to restore previous settings.
   - **Edit If** to add or delete this zone filter to/from an interface. The **Add/Delete Interface to Zone Filter** dialog box opens. See "Adding or Deleting Interfaces to a Zone Filter", later in this section for more information.

Editing an AppleTalk Zone Filter Using the CLI

To edit an AppleTalk zone filter using the CLI, enter the following command from **Configure** mode:

```
> (config-if <interface-name>:)# appletalk
access-list <access-list-number>
<permit|deny> zone <string>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Adding or Deleting Interfaces to a Zone Filter

You can add or delete interfaces to a zone filter using either the web agent or the CLI.

Adding or Deleting Interfaces to a Zone Filter Using the Web Agent

To add or delete interfaces to a zone filter using the web agent:

1. Select **Zone Filter** from the **Routing > AppleTalk > Configuration** group on the web agent window. The **AppleTalk Zone Filter** dialog box opens (Figure 15-11).
2. Select **Edit If**. The **Add/Delete Interface to Zone Filter** dialog box opens (Figure 15-13).

Figure 15-13. Add/Delete Interface to Zone Filter Dialog Box

3. Select the interface to be added from the **Add** field pull-down menu.

   Or

   Click the checkbox in the **Select** column for the interface that you want to be remove.

4. Click ...

   — **Add** to add this zone filter to the selected interface.

   — **DELETE** to remove this zone filter from the selected interface.

   — **CANCEL** to restore previous settings.

Adding or Deleting Interfaces to a Zone Filter Using the CLI

To add interfaces to a zone filter using the CLI, enter the following command from **Configure** mode:

```
> (config-if <interface-name>:)# appletalk
access-list <access-list-number>
<permit|deny> zone <string>
```

To delete interfaces to an zone filter, enter the following command from **Configure** mode:

```
> (config-if <interface-name>:)# no appletalk
access-list <access-list-number> <permit|deny>
zone <string>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing AppleTalk Statistics

This section includes:

- Viewing AppleTalk Global Statistics
- Viewing the AppleTalk Interface Statistics Table
- Viewing the AppleTalk Interface Statistics Table Using the CLI
- Viewing AppleTalk Route Table Statistics
- Viewing the AppleTalk ARP Cache Table
- Viewing the AppleTalk Zone Table
- Viewing AppleTalk Zone Table Statistics
- Viewing the AppleTalk NBP Table

Viewing AppleTalk Global Statistics

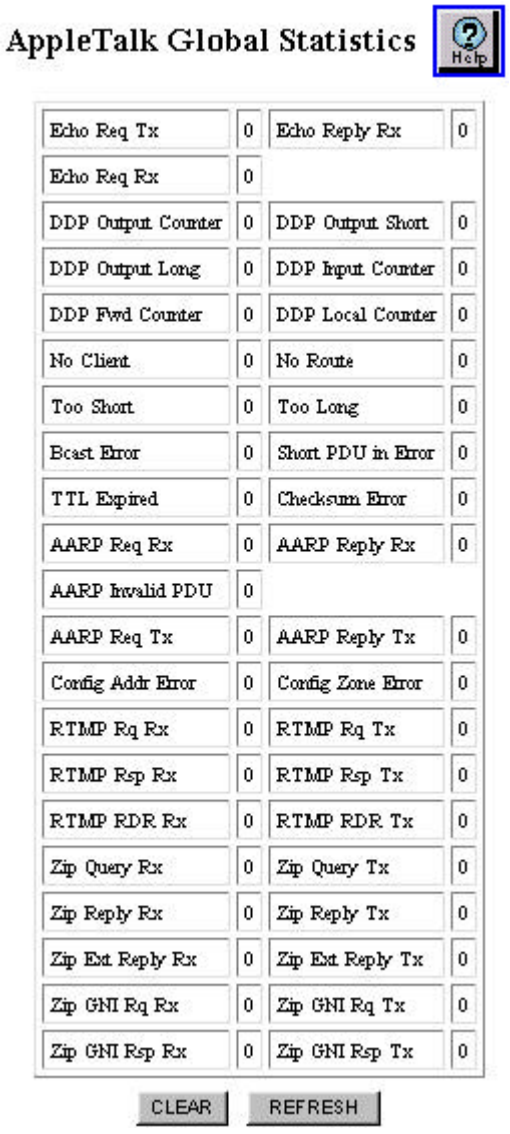
You can view AppleTalk global statistics using either the web agent or the CLI.

Viewing AppleTalk Global Statistics Using the Web Agent

To view AppleTalk global statistics using the web agent:

1. Select **Global Statistics** from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk Global Statistics** dialog box opens (Figure 15-14).

Figure 15-14. AppleTalk Global Statistics Dialog Box


AppleTalk Global Statistics
Help
Echo Req Tx 0 Echo Reply Rx 0
Echo Req Rx 0
DDP Output Counter 0 DDP Output Short 0
DDP Output Long 0 DDP Input Counter 0
DDP Fwd Counter 0 DDP Local Counter 0
No Client 0 No Route 0
Too Short 0 Too Long 0
Bcast Error 0 Short PDU in Error 0
TTL Expired 0 Checksum Error 0
AARP Req Rx 0 AARP Reply Rx 0
AARP Invalid PDU 0
AARP Req Tx 0 AARP Reply Tx 0
Config Addr Error 0 Config Zone Error 0
RTMP Rq Rx 0 RTMP Rq Tx 0
RTMP Rsp Rx 0 RTMP Rsp Tx 0
RTMP RDR Rx 0 RTMP RDR Tx 0
Zip Query Rx 0 Zip Query Tx 0
Zip Reply Rx 0 Zip Reply Tx 0
Zip Ext Reply Rx 0 Zip Ext Reply Tx 0
Zip GNI Rq Rx 0 Zip GNI Rq Tx 0
Zip GNI Rsp Rx 0 Zip GNI Rsp Tx 0
CLEAR
REFRESH

2. Refer to Table 15-5 for information about the **AppleTalk Global Statistics** dialog box parameters.

Table 15-5. AppleTalk Global Statistical Dialog Box Parameters

Parameter	Number of...
Echo Req Tx	Echo requests transmitted.
Echo Reply Rx	Echo replies received.
Echo Req Rx	Echo requests received.
DDP Output Counter	DDP packets sent from this node.
DDP Output Short	DDP packets sent using the short format.
DDP Output Long	DDP packets sent using the long format.
DDP Input Counter	DDP packets received at this node.
DDP Fwd Counter	DDP packets forwarded through this node.
DDP Local Counter	DDP packets received destined for this node.
No Client	Packets received for which the destination socket was not known.
No Route	Packets received for which the destination route was not known.
Too Short	Packets received that were smaller than the minimum size allowed for an AppleTalk packet.
Too Long	Packets received that were larger than the minimum size allowed for an AppleTalk packet.
Bcast Error	Broadcast errors detected.
Short PDU in Error	Packets received that had a short PDU in error.
TTL Expired	Packets dropped because they timed out.
Checksum Error	Packets which had checksum in error.
AARP Req Rx	AppleTalk ARP requests received.
AARP Reply Rx	Appletalk ARP replies received.
AARP Invalid PDU	AppleTalk ARP requests received which were invalid.
AARP Req Tx	AppleTalk ARP requests transmitted.
AARP Reply Tx	AppleTalk ARP replies transmitted.

Table 15-5. AppleTalk Global Statistical Dialog Box Parameters continued

Parameter	Number of...
Config Addr Error	Configuration address errors detected.
Config Zone Error	Zone configuration errors detected.
RTMP Rq Rx	RTMP requests received.
RTMP Rq Tx	RTMP requests transmitted.
RTMP Rsp Rx	RTMP responses received.
RTMP Rsp Tx	RTMP responses transmitted.
RTMP RDR Rx	RTMP route data requests received.
RTMP RDR Tx	RTMP route data requests transmitted.
Zip Query Rx	ZIP queries received.
Zip Query Tx	ZIP queries transmitted.
Zip Reply Rx	ZIP replies received.
Zip Reply Tx	ZIP replies transmitted.
Zip Ext Reply Rx	ZIP extended replies received.
Zip Ext Reply Tx	ZIP extended replies transmitted.
Zip GNI Rq Rx	ZIP get net info request received.
Zip GNI Rq Tx	ZIP get net info request transmitted.
Zip GNI Rsp Rx	ZIP get net info response received.
Zip GNI Rsp Tx	ZIP get net info response transmitted.

3. Click **REFRESH** to update all statistics.

   Or

   Click **CLEAR** to reset all statistics to zero.

Viewing AppleTalk Global Statistics Using the CLI

To view AppleTalk global statistics using the CLI, enter the following command:

```
>#  show appletalk globals
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing the AppleTalk Interface Statistics Table

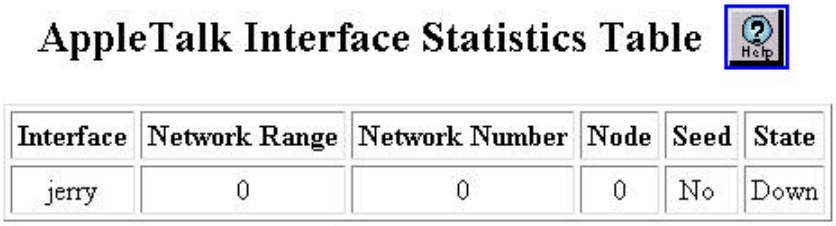
You can view the AppleTalk interface statistics table using either the web agent or the CLI.

Viewing the AppleTalk Interface Statistics Table Using the Web Agent

To view the AppleTalk Interface statistics table using the web agent:

1. Select **Interface Statistics**.from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk Interface Statistics Table** opens (Figure 15-15).

Figure 15-15. AppleTalk Interface Statistics Table



2. Refer to Table 15-6 for information on the **AppleTalk Interface Statistics Table** parameters**:**

Table 15-6. AppleTalk Interface Statistics Table Parameters

Parameter	Definition
Interface	Displays the name of the AppleTalk interface.
Network Range	Displays the network range associated with the AppleTalk interface.
Network Number	Displays the network number of this node.
Node	Displays the node number of this node.
Seed	Displays whether the AppleTalk interface seeded the network.
State	Displays the state of the AppleTalk interface. The options include: • **Up** - indicates that the AppleTalk interface is active. • **Down** - indicates that the AppleTalk interface is inactive.

Viewing the AppleTalk Interface Statistics Table Using the CLI

To view the AppleTalk Interface statistics table using the CLI, enter the following command from **Priv** mode:

```
># show appletalk interface brief <CR>|<interface-name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing the AppleTalk Route Table

You can view the AppleTalk route table using the web agent or the CLI. You can also delete single entries from the table, or flush all of the routes from the table.

Viewing the AppleTalk Route Table Using the Web Agent

To view the AppleTalk route table, and delete or flush entries from the table using the web agent:

1. Select **Route Table** from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk Route Table** opens (Figure 15-16).

Figure 15-16. AppleTalk Route Table Window

2. Refer to Table 15-7 for information about the **AppleTalk Route Table** parameters:

Table 15-7. AppleTalk Route Table Parameters

Parameter	Definition
Select	Select the entry to be acted upon.
Network Range	Displays the network range.
Metric	Displays the AppleTalk metric for the network range.
State	Displays the state of the entry.The options include: • Good • Suspect • Going Bad • Bad
Owner	Displays the AppleTalk component responsible for the addition of the route.The options include: • Local • Static • RTMP
Next Hop	Displays the next hop address where forwarded packets are routed.
Interface	Displays the Appletalk interface associated with the route table entry.
Zones	Displays the zones associated with the selected AppleTalk route.

3. Click **Delete Entries** to remove selected route table entries.

   Or

   Click **Flush Route Table** to empty the route table of all dynamic entries. Static and Local entries are not flushed.

Viewing the AppleTalk Interface Statistics Table Using the CLI

To view the AppleTalk Interface statistics table using the CLI, enter the following command:

```
>#  show appletalk route
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing AppleTalk Route Table Statistics

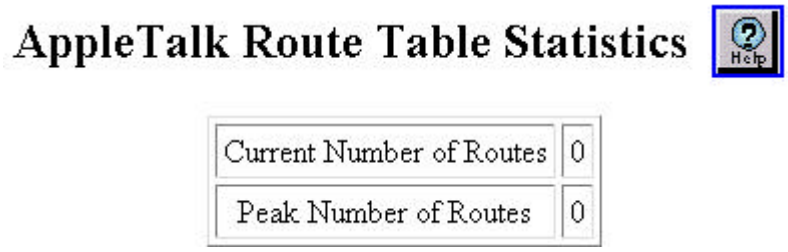
You can view AppleTalk route table statistics using either the web agent or the CLI.

Viewing AppleTalk Route Table Statistics Using the Web Agent

To view AppleTalk route table statistics using the web agent:

1. Select **Route Table Statistics** from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk Route Table Statistics** dialog box opens (Figure 15-17).

Figure 15-17. AppleTalk Route Table Statistics Dialog Box



2. Refer to Table 15-8 for information on **AppleTalk Route Table Statistics** dialog box parameters:

Table 15-8. AppleTalk Route Table Statistics Dialog Box Parameters

Parameter	Definition
Current Number of Routes	Displays the current number of AppleTalk routes.
Peak Number of Routes	Displays the peak number of AppleTalk routes.

Viewing AppleTalk Route Table Statistics Using the CLI

To view AppleTalk route table statistics using the CLI, enter the following command:

```
>#  show appletalk route <cr|starting-range>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing the AppleTalk ARP Cache Table

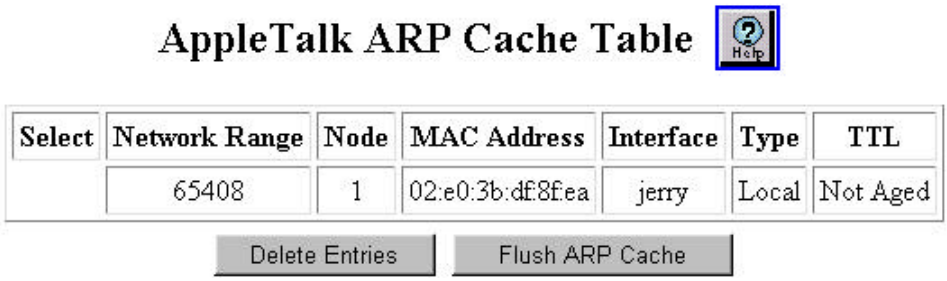
You can view the AppleTalk ARP cache table using either the web agent or the CLI.

Viewing the AppleTalk ARP Cache Table Using the Web Agent

To view the AppleTalk ARP cache table using the web agent:

1. Select **ARP Table** from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk ARP Cache Table** opens (see Figure 15-).

Figure 15-18. AppleTalk ARP Cache Table



2. Refer to Table 15-9 for a definition of the **AppleTalk ARP Cache Table** parameters.

Table 15-9. AppleTalk ARP Cache Table Parameters

Parameter	Definition
Select	Select the table entry to be acted upon.
Network Range	Displays the network range.
Node	Displays the node number for the entry.
MAC Address	Displays the MAC address associated with the AppleTalk ARP cache table entry of the node.
Interface	Displays the AppleTalk interface associated with the AppleTalk ARP cache table entry.
Type	Displays the type of cache entries.The values are: • Local • Broadcast • Dynamic • Router Neighbor
TTL	Displays the time-to-live value for the selected AppleTalk ARP cache table entry. Local and Broadcast entries do not time out.

3. Select the checkbox next to any specific ARP entries that you want to delete and click **Delete Entries**.

   or

   Click **Flush Route Table** to reset the ARP cache table entries. Only Dynamic and Router Neighbor entries are flushed.

Viewing the AppleTalk ARP Cache Table Using the CLI

To view the AppleTalk ARP cache table using the CLI, enter the following command from **User** mode:

```
>show appletalk arp [all]
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing the AppleTalk Zone Table

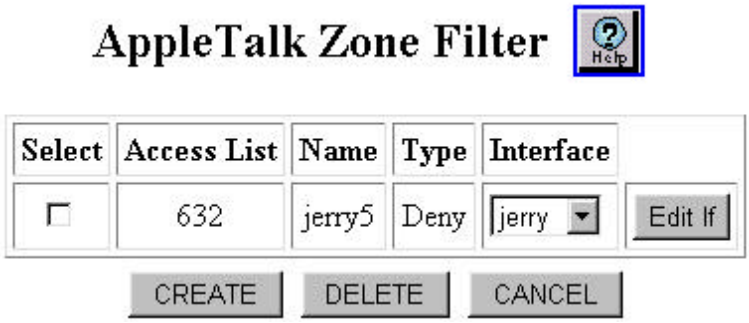
You can view the AppleTalk Zone table using either the web agent or the CLI.

Viewing the AppleTalk Zone Table Using the Web Agent

To view the AppleTalk zone table using the web agent:

1. Select **Zone Table** from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk Zone Table** opens (Figure 15-19).

Figure 15-19. AppleTalk Zone Table



2. Refer to Table 15-10 for an explanation of the **AppleTalk Zone Table** parameters.

Table 15-10. AppleTalk Zone Table Parameters

Parameter	Definition
Index	Displays the zone index.
Name	Displays the zone name.
Network Range	Displays the network range associated with the zone.

Viewing the AppleTalk Zone Table Using the CLI

To view the AppleTalk zone table using the CLI, enter the following command from **User** mode:

```
># show appletalk zone
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing AppleTalk Zone Table Statistics

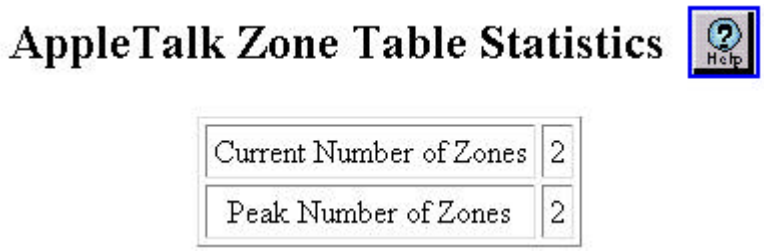
You can view the AppleTalk Zone Table Statistics using either the web agent or the CLI.

Viewing AppleTalk Zone Table Statistics Using the Web Agent

To view AppleTalk zone table statistics using the web agent:

1. Select **Zone Table Statistics** from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk Zone Table Statistics** table opens (Figure 15-20).

Figure 15-20. AppleTalk Zone Table Statistics Table



2. Refer to Table 15-11 for an explanation of the **AppleTalk Zone Table Statistics** parameters.

Table 15-11. AppleTalk Zone Table Statistical Parameters

Parameter	Definition
Current Number of Zones	Displays the current number of AppleTalk zones.
Peak Number of Zones	Displays the peak number of AppleTalk zones.

Viewing AppleTalk Zone Table Statistics Using the CLI

To view AppleTalk zone table statistics using the CLI, enter the following command from **User** mode:

```
> # show appletalk zone <cr|zone-name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing the AppleTalk NBP Table

You can view the AppleTalk NBP Table using either the web agent or the CLI.

Viewing the AppleTalk NBP Table Using the Web Agent

To view the AppleTalk NBP table using the web agent:

1. Select **Zone Table** from the **Routing > AppleTalk > Display** group on the web agent window. The **AppleTalk Zone Table** opens (Figure 15-19).

2. Refer to Table 15-12 for an explanation of the AppleTalk NBP Table parameters:

Table 15-12. AppleTalk NBP Table Statistical Parameters

Parameter	Definition
Index	Displays the index of the name binding protocol entry.
Name	Displays the name of the NBP entry.
Type	Displays the type of object named.
Interface	Displays the AppleTalk interface associated with the AppleTalk NBP table entry.
Zone	Displays the zone field associated with the NBP table entry.

Viewing the AppleTalk NBP Table Using the CLI

To view the AppleTalk NBP table using the CLI, enter the following command from **User** mode:

```
> show appletalk nbp <cr|nbp-name>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

16 Managing Intelligent Multicasting

Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- Introduction
- Configuring Global Intelligent Multicasting
- Displaying Router Ports
- Configuring Static Router Ports
- Searching for Intelligent Multicast Sessions
- Creating a Static Multicast Session
- Configuring Internet Group Management Protocol (IGMP) Snooping (Multilayer only)
- Configuring the Lucent Group Management Protocol (LGMP) Server
- Configuring/Viewing an LGMP Client
- Enabling/Viewing Cisco Group Management Protocol (CGMP) Snooping

Introduction

Intelligent multicasting refers to the forwarding of layer 2 multicast traffic (packets with a multicast destination MAC address) to a subset of ports participating in a VLAN. It limits the forwarding of layer 2 multicast traffic to only those ports on the VLAN with clients that want to receive this multicast traffic.

When disabled, intelligent multicasting floods layer 2 multicast traffic to all ports on the VLAN on which the traffic is received.

A multicast session is layer 2 multicast traffic on a VLAN. The switch supports 60 sessions per VLAN.

A client port is a port with an attached host configured to receive a multicast session.

Router ports are ports that are attached to (or in the path to) multicast routers and must be treated specially. All multicast traffic on a VLAN must be forwarded to the router.

You can manually create and delete multicast sessions through the user configuration. The addition of client and router ports can also be performed manually. Dynamic intelligent multicasting is achieved through Internet Group Management Protocol (IGMP) snooping, Lucent Group Membership Protocol (LGMP), or Cisco Group Management Protocol (CGMP) snooping. All of these mechanisms are based on the assumption that the client host is running IGMP, requesting membership in the IP multicast session.

*** Note:** If there is no multicast session created for a multicast flow in a VLAN, then that multicast flow will be flooded to all ports on the VLAN. Intelligent multicasting must be enabled for any dynamic intelligent multicasting to be active.

Layer 3 Dynamic Intelligent Multicasting

IGMP snooping is supported for VLANs that have IGMP interfaces enabled. This is the recommended means of supporting dynamic intelligent multicasting in layer 3. For all VLANs that do not have an IGMP interface enabled, the layer 2 dynamic intelligent multicasting mechanisms (LGMP client and CGMP snooping) are supported.

*** Note:** For layer 2 or layer 3 LGMP to perform properly, VLAN IDs must match between switches. Specifically, if two switches are connected with a non-tagging link, the port-default VLANs of the ports connecting the two switches must be the same. This is because the VLAN is embedded in the LGMP message; and the receiving switch maps the LGMP message to the specified VLAN.

IGMP Snooping

IGMP snooping is only supported in layer 3. As IGMP reports are received by the switch, IGMP sessions are created. Intelligent multicast sessions are created and the ports on which these reports are received are added to the appropriate sessions. When the IGMP session is terminated, the associated intelligent multicast session is deleted.

*** Note:** IGMP snooping is only available for VLANs that have an IGMP interface enabled.

LGMP Server

Because layer 2 cannot snoop IGMP messages, it requires layer 3 to provide the necessary information through a Lucent proprietary protocol, Lucent Group Membership Protocol (LGMP).

Essentially, LGMP works by having the layer 3 switch re-transmit received IGMP messages to the layer 2 switches by sending them to a well known multicast MAC address. The layer 2 switch then creates multicast sessions, adds clients to those sessions, and removes sessions dynamically, as if it were directly receiving the IGMP messages.

If more than one LGMP server is on a VLAN, one server will be elected as the *distributor*. Only the distributor disseminates intelligent multicasting information using LGMP packets.

*** Note:** IGMP snooping must be enabled for LGMP server availability. An LGMP server is active only for VLANs that have an IGMP interface enabled.

Layer 2 Dynamic Intelligent Multicasting

Layer 2 does not support IGMP snooping to dynamically configure intelligent multicast sessions. Therefore, LGMP client or CGMP snooping is used to achieve dynamic intelligent multicasting.

LGMP Client

An LGMP server disseminates multicast session information using LGMP. An LGMP client creates multicast sessions, adds clients to those sessions, and removes sessions dynamically, using the information sent from the LGMP server.

CGMP Snooping

Cisco routers disseminate multicast session information via the CGMP protocol. The switch has the ability to listen to these messages and dynamically create multicast sessions, add client ports to those sessions, and remove sessions.

Pruning Dynamic Sessions, Client Ports, and Router Ports

Normally, dynamically created multicast sessions are removed by the application (for example, IGMP Snooping, LGMP, or CGMP Snooping) that created the session when the session is no longer active. You can also enable Automatic Session Pruning so that if a session has not been active for Session Pruning Time, it is automatically removed.

You also have the ability to enable Automatic Client Port Pruning so that a client port is removed from a session if no IGMP reports have been received on that port for that session in the time specified.

*** Note:** By enabling Automatic Client Port Pruning, there is a chance that the switch may disrupt multicast service temporarily to clients requesting to receive that multicast traffic.

Automatic Router Port Pruning works similarly pruning *quiet* router ports. If the switch has not been notified that there is a router on the port in Router Pruning Time, then the router port is removed.

Configuring Intelligent Multicasting

This section provides the following procedures:

- Configuring Global Intelligent Multicasting
- Displaying Router Ports
- Configuring Static Router Ports
- Searching for Intelligent Multicast Sessions
- Deleting an Intelligent Multicast Session
- Deleting a Multicast Session Client Port
- Creating a Static Multicast Session
- Deleting Static Multicast Sessions
- Creating Static Client Ports
- Deleting Static Client Ports

Configuring Global Intelligent Multicasting

You can configure intelligent multicasting globally using either the web agent or the CLI.

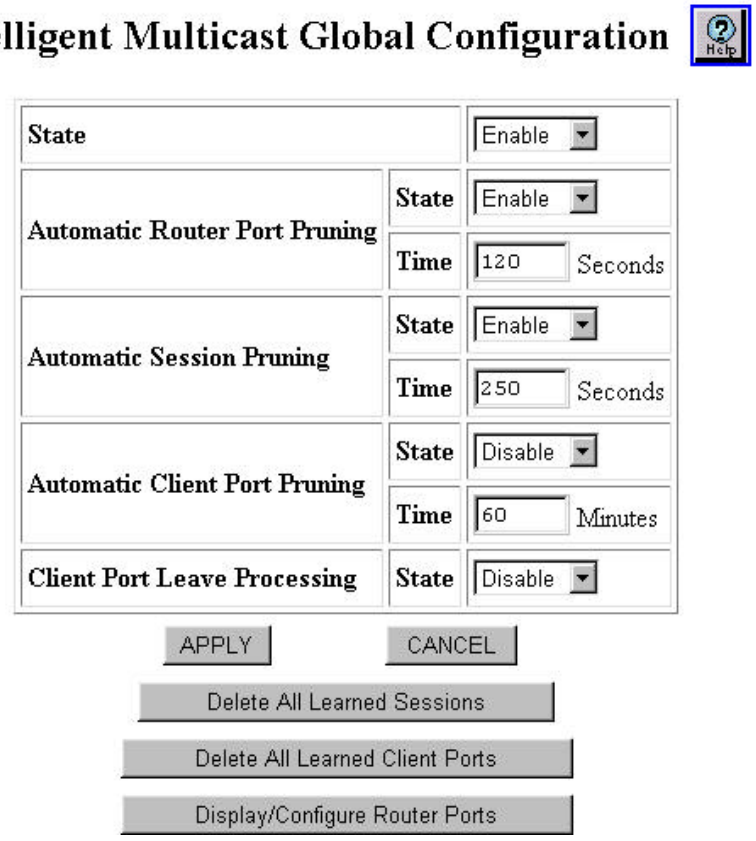
Configuring Global Intelligent Multicasting Using the Web Agent

To configure intelligent multicasting globally using the web agent:

1. Select Global Configuration from the Layer 2 Switching > Intelligent Multicast group on the web agent window. The Intelligent Multicast Global Configuration dialog box opens (Figure 16-1).

*** Note:** You cannot delete Static sessions and client ports from this dialog box. Refer to "Deleting a Multicast Session Client Port" and "Deleting Static Multicast Sessions", in this chapter to delete static sessions and client ports.

Figure 16-1. Intelligent Multicasting Global Configuration Dialog Box



***Note:** You must enable IP multicast forwarding on a layer 3 switch. Refer to "Enabling IP Routing", in Chapter 9, Configuring IP Routing.

2. Refer to Table 16-1 to configure the Intelligent Global Multicast Configuration dialog box parameters:

Table 16-1. Intelligent Global Multicast Configuration Dialog Box Parameters

Parameter	Definition
Enable State	Select **Disable** to prevent intelligent multicasting globally. The default value is **Enabled**.
Automatic Router Port Pruning	Select: • **Disable** - to prevent automatic router port pruning. The default value is **Enable**. • **Time** - Enter the time, in seconds, after which quiet learned router ports can be pruned. The valid range (in seconds) is 10 to 172800 (48 hours). The default value is **120 seconds**.
Automatic Session Pruning	Select: • **Disable** - to remove stale learned sessions. The default value is **Enable**. • **Time** - Enter the time, in seconds, after which stale learned sessions can be removed. The valid range (in seconds) is 10 to 172800 (48 hours). The default value is **250 seconds**.
Automatic Client Port Pruning	Select: • **Disable** - to prevent the automatic removal of quiet learned client ports from a session. The default value is **Enable**. • **Time** - Enter the time, in minutes, after which quiet learned client ports can be automatically removed from a session. The valid range (in minutes) is 1 to 1440 (24 hours). The default value is **60 minutes**.

3. Click ...:

   — APPLY to save your changes.

   — CANCEL to restore previous settings.

   — Delete All Learned Sessions to remove all learned multicast sessions.

   — Delete All Learned Client Ports to remove all learned client ports from all multicast sessions.

   — Display/Configure Router Ports to display the router ports and configure your static router ports.

Configuring Global Intelligent Multicasting Using the CLI

To configure intelligent multicasting globally using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set intelligent-multicast
{enable}
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Displaying Router Ports

You can display router ports using either the web agent or the CLI.

Displaying Router Ports Using the Web Agent

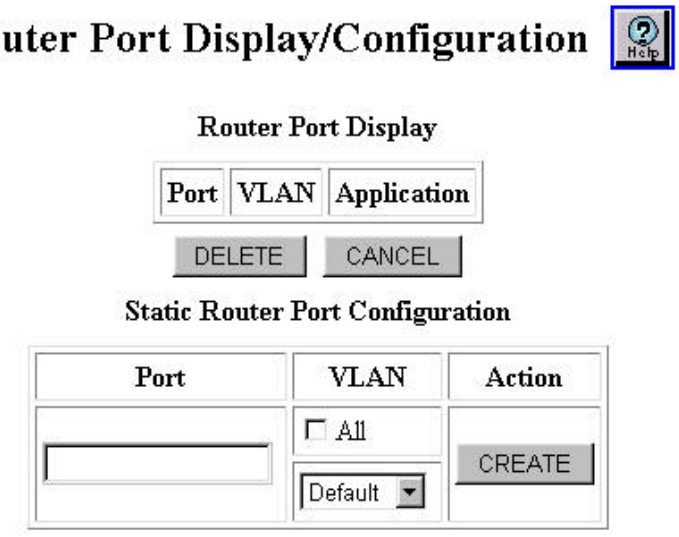
To display router ports using the web agent:

1. Select Global Configuration from the L2 Switching > Intelligent Multicast group on the web agent window. The Intelligent Multicast Global Configuration dialog box opens (Figure 16-1).

   ***Note:** You must enable intelligent multicasting on a global basis to make your router ports active. See "Configuring Global Intelligent Multicasting", earlier in this chapter.

2. Select Display/Configure Router Ports. The Router Port Display/Configuration dialog box opens (Figure 16-2).

Figure 16-2. Router Port Display/Configuration Dialog Box



3. Refer to Table 16-2 for an explanation of the Router ports.

Table 16-2. Router Port Display/Configuration Dialog Box Parameters

Parameter	Definition
Port	Displays the router port in the multicast session.
VLAN	Displays the port VLAN of the router.
Application	Displays the active applications of the router port. The applications include: • Mgmt (Static) • IGMP • LGMP • CGMP

4. Select a router port from the Port column and click DELETE to delete the port, or CANCEL to restore previous settings.

Displaying Router Ports Using the CLI

To display router ports using the CLI, enter the following command from Priv mode:

```
cajun# show intelligent-multicast router-port
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring Static Router Ports

You can configure Static Router ports using either the web agent or the CLI.

Configuring Static Router Ports Using the Web Agent

To configure a static router port using the web agent:

1. Select Global Configuration from the L2 Switching > Intelligent Multicast group on the web agent window. The Intelligent Multicast Global Configuration dialog box opens (Figure 16-1).

***Note:** You must enable intelligent multicasting on a global basis to make your static router port configuration active. See "Configuring Global Intelligent Multicasting", earlier in this chapter.

2. Select Display/Configure Router Ports. The Router Port Display/Configuration dialog box opens (Figure 16-2).

3. Enter a port number in the Port field.

4. Select All from the VLAN column to add this router port to all VLANs

   Or

   Select a specific VLAN from the VLAN field pull-down menu.

   ***Note:** When adding a router port to all VLANs, the router port is added only to the VLANs bound to the switch port. To bind multiple VLANs to a switch port, refer to *Chapter 4*, *Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping*, earlier in this guide.

5. Click CREATE to save your changes.

Configuring Static Router Ports Using the CLI

To configure a static router port using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set intelligent-multicast
static-client-port <group-address>|<mac-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Searching for Intelligent Multicast Sessions

You can search for intelligent multicast sessions using either the web agent or the CLI.

Searching for Intelligent Multicast Sessions Using the Web Agent

To perform a session search using the web agent:

1. Select Session Search from the L2 > Intelligent Multicast group on the web agent window. The Intelligent Multicast Session Search dialog box opens (Figure 16-3).

Figure 16-3. Intelligent Multicast Session Search Dialog Box

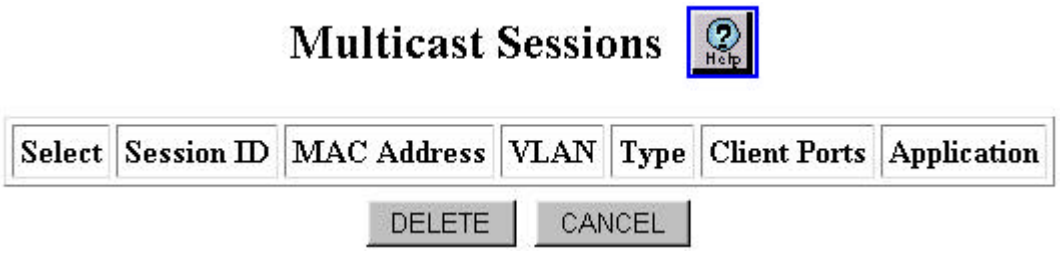
2. Refer to Table 2 for an explanation of the Intelligent Multicast Session Search dialog box parameters:i

Table 16-3. Intelligent Multicast Session Search Dialog Box Parameters

Search By Parameter:	Search Value:
IP Subnet	• I**P Address** - enter the IP address on which you want to perform a search • **IP Address Mask** - Enter the associated IP Address mask
MAC Address	Enter the MAC address on which you want to perform a search
VLAN	Select a VLAN from the pull-down menu on which you want to perform a search.
Client Port	Enter a client port number on which you want to perform a search.
Session Type	Select a Session Type from the pull-down menu on which you want to perform a search. The options are Learned and Mgmt.

3. Select SEARCH to begin the search for the multicast session. The Multicast Sessions dialog box opens with the search results (Figure 16-4).

Figure 16-4. Multicast Sessions Dialog Box



4. Refer to Table 16-4 for an explanation of the Multicast Sessions dialog box parameters:

Table 16-4. Multicast Sessions Dialog Box Parameters

Parameter	Definition
Select	Select the multicast session.
Session ID	Displays the multicast session identifier.
MAC Address	Displays the MAC address of the multicast session.
VLAN	Displays the VLAN on which the multicast session exists.
Type	Displays the type of multicast session. Options include: • **Learned** - Entry is dynamically learned. • **Mgmt** - Entry is configured statically by the user.
Client Ports	Displays the number of client ports in the multicast session and opens the Multicast Session Client Ports dialog box.
Application	Displays the active application(s) of the multicast session. The applications include: • Mgmt • IGMP • LGMP • CGMP

Searching for Intelligent Multicast Sessions Using the CLI

To perform a session search using the CLI, enter the following command from User mode:

```
cajun# show intelligent-multicast session
<options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting an Intelligent Multicast Session

You can delete an intelligent multicast session using either the web agent or the CLI.

Deleting an Intelligent Multicast Session Using the Web Agent

To delete an intelligent multicast session using the web agent:

1. Select Session Search from the L2 > Intelligent Multicast group on the web agent window. The Intelligent Multicast Session Search dialog box opens (Figure 16-3).
2. Select SEARCH to begin the search for the multicast session. The Multicast Sessions dialog box opens with the search results (Figure 16-4).
3. Select the checkbox next to the multicast session that you want to delete and click DELETE.

***Note:** Static (Mgmt) sessions can only be deleted through the Static Sessions dialog box.

Deleting a Multicast Session Using the CLI

To delete a multicast session client port using the CLI, enter the following command from Configure mode:

```
cajun(configure)# clear intelligent-multicast
session <session-id>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting a Multicast Session Client Port

You can delete an intelligent multicast session client port for either the web agent or the CLI.

Deleting a Multicast Session Client Port Using the Web Agent

To delete a multicast session client port using the web agent:

1. Select Session Search from the L2 > Intelligent Multicast group on the web agent window. The Intelligent Multicast Session Search dialog box opens (Figure 16-3).
2. Select the client port number from the Client Ports column. The Multicast Session Client Port dialog box opens.
3. Refer to Table 16-5 for an explanation of the Multicast Session Client Port dialog box parameters:

Table 16-5. Multicast Session Client Port Dialog Box Parameters

Parameter	Definition
Select	Select the multicast session client port.
Port	Displays the client port number.
Application	Displays the application(s) associated with this client port. The applications are: • Mgmt • IGMP • LGMP • CGMP

4. Click DELETE to remove your selected multicast session client port, or CANCEL to restore previous settings.

*** Note:** Static (Mgmt) client ports can only be removed through the Static Sessions dialog box.

Deleting a Multicast Session Client Port Using the CLI

To delete a multicast session client port using the CLI, enter the following command from Configure mode:

```
cajun(configure)# clear intelligent-multicast
client-port <session-id>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating a Static Multicast Session

You can create a static multicast session using either the web agent or the CLI.

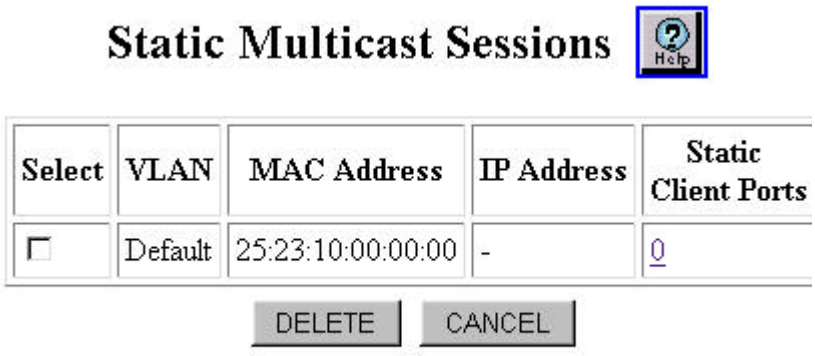
Creating a Static Multicast Session Using the Web Agent

To create a new static multicast session using the web agent:

1. Select Static Sessions from L2 > Intelligent Multicast group on the web agent window. The Static Multicast Sessions dialog box opens (Figure 16-5).

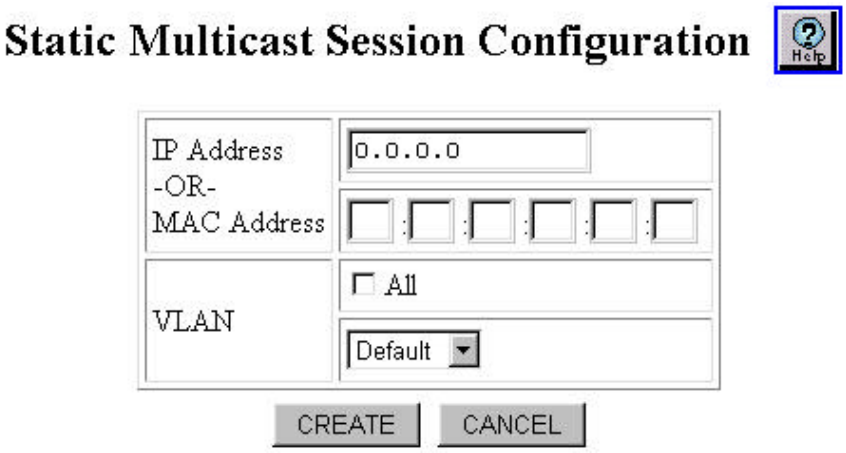
   ***Note:** You must enable intelligent multicasting on a global basis to make your static multicast session active. See "Configuring Global Intelligent Multicasting", earlier in this chapter.

Figure 16-5. Static Multicast Sessions Dialog Box



2. Select **Create New Session**. The **Static Multicast Session Configuration** dialog box opens (Figure 16-6).

Figure 16-6. Static Multicast Session Configuration Dialog Box



3. Configure the Static Multicast Session Configuration dialog box parameters (refer to Table 16-6):

Table 16-6. Static Multicast Session Configuration Dialog Box Parameters

Parameter	Definition
IP Address	Enter the IP address of the new static multicast session. The range must be between 224.0.1.0 to 239.255.255.255.
MAC Address	Enter the MAC address of the new static multicast session. Specifying the MAC address is not used for an IP multicast session.
VLAN	Enter the VLAN associated with the new multicast session. Click All to add all VLANs to the multicast session, or select a specific VLAN from the pull-down menu.

4. Click CREATE to create the new static multicast session, or CANCEL to restore previous settings.

Creating a Static Multicast Session Using the CLI

To create a new static multicast session using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set intelligent-multicast
session <group-address|mac-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting Static Multicast Sessions

You can delete static multicast sessions using either the web agent or the CLI.

Deleting Static Multicast Sessions Using the Web Agent

To delete a static multicast session using the web agent:

1. Select Static Sessions from L2 > Intelligent Multicast group on the web agent window. The Static Multicast Sessions dialog box opens (Figure 16-5).

2. Refer to Table 16-7 for an explanation of the Static Multicast Sessions dialog box parameters (Figure 16-7):

Figure 16-7. Static Multicast Sessions Dialog Box

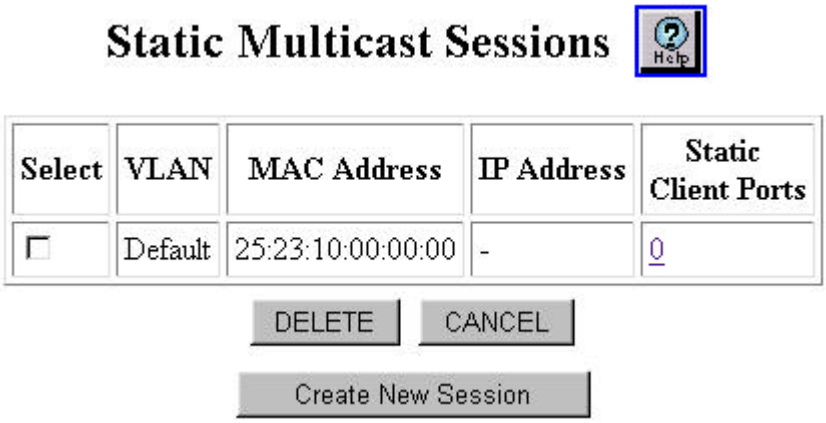


Table 16-7. Static Multicast Sessions Dialog Box Parameters

Parameter	Definition
Select	Select the static multicast session to be modified.
VLAN	Displays the VLAN on which the static multicast session exists.
MAC Address	Displays the MAC address of the static multicast session.
IP Address	Displays the IP address associated with the static multicast session, if available.
Static Client Ports	Displays the number of static client ports associated with the static multicast session and opens the Static Multicast Session Client Ports dialog box.

3. Select the checkbox next to the static multicast session that you want to delete.

4. Click DELETE to remove the static multicast session, or CANCEL to ignore the operation.

Deleting Static Multicast Sessions Using the CLI

To delete a static multicast session using the CLI, enter the following command from Configure mode:

```
cajun(configure)# clear intelligent-multicast
session <session-id>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Creating Static Client Ports

You can create and add static client ports using either the web agent or the CLI.

*** Note:** You can only add static client ports to static sessions on VLANs that the port is bound to or on sessions created for All VLANs.

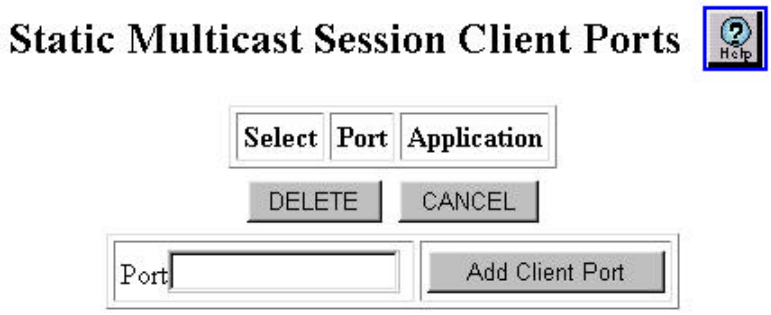
Creating Static Client Ports Using the Web Agent

To create a static client port using the web agent:

1. Select Static Sessions from L2 > Intelligent Multicast group on the web agent window. The Static Multicast Sessions dialog box opens (Figure 16-5).

2. Select the number from the Static Client Ports column. The Static Multicast Sessions Client Ports dialog box opens (Figure 16-8).

Figure 16-8. Static Multicast Sessions Clients Port Dialog Box



3. Enter the new port number to be added in the Port field,.

4. Click Add Client Port. The new port is added.

Creating Static Client Ports Using the CLI

To create a static client port using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set intelligent-multicast
static-client-port <group-address|mac-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Deleting Static Client Ports

You can delete static client ports from either the web agent or the CLI.

Deleting Static Client Ports Using the Web Agent

To delete static client ports using the web agent:

1. Select Static Sessions from L2 > Intelligent Multicast group on the web agent window. The Static Multicast Sessions dialog box opens (Figure 16-5).
2. Select the number from the Static Client Ports column. The Static Multicast Sessions Client Ports dialog box opens (Figure 16-8).
3. Select a port and click DELETE to remove the static client port, or CANCEL to restore previous settings.

Deleting Static Client Ports Using the CLI

To delete static client ports using the CLI, enter the following command from Configure mode:

```
cajun(configure)# clear intelligent-multicast
static-client-port <group-address|mac-address>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring Internet Group Management Protocol (IGMP) Snooping (Multilayer only)

This section provides the following procedures:

- Enabling IGMP Snooping
- Configuring IGMP Snooping

Enabling IGMP Snooping

You can enable IGMP snooping using either the web agent or the CLI.

Enabling IGMP Snooping Using the Web Agent

To enable IGMP Snooping using the web agent:

1. Select IGMP Snooping from the L2 > Intelligent Multicast group on the web agent window. The IGMP Snooping dialog box opens (Figure 16-9).

*** Note:** IGMP snooping only works on VLANS that have an IGMP interface enabled. You must also enable intelligent multicasting on a global basis.

Figure 16-9. IGMP Snooping Dialog Box

2. Select Enable from the State field.
3. Click Apply to complete the operation or Cancel to ignore the operation.

Enabling IGMP Snooping Using the CLI

To enable IGMP Snooping using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set igmp-snooping enable
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring IGMP Snooping

You can configure IGMP snooping using either the web agent or the CLI.

Configuring IGMP Snooping Using the Web Agent

To configure IGMP snooping using the Web Agent:

1. Select IGMP Snooping from the L2 > Intelligent Multicast group on the web agent window. The IGMP Snooping dialog box opens (Figure 16-9).

2. Refer to Table 16-8 for an explanation of the IGMP Snooping dialog box parameters:

Table 16-8. IGMP Snooping Dialog Box Parameters

Parameter	Definition
Enable State	Select **Enable** to allow the IGMP snooping on the interface. The default value is **Disable**.
Intelligent Multicast Session Statistics	• **New Sessions Created** - Displays the number of new sessions created by IGMP snooping. • **Sessions Destroyed** - Displays the number of sessions removed by IGMP snooping. • **New Client Ports Added** - Displays the number of new client ports added by IGMP snooping. • **New Router Ports Added** - Displays the number of new router ports added by IGMP snooping. • **Router Ports Removed** - Displays the number of router ports removed by IGMP snooping.

3. Click ...:
   - — APPLY to save your changes.
   - — CANCEL to restore previous settings.
   - — CLEAR to clear the statistics.
   - — REFRESH to refresh the contents of the table.

Configuring IGMP Snooping Using the CLI

To configure IGMP snooping using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set igmp-snooping enable
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring the Lucent Group Management Protocol (LGMP) Server

The section provides the following procedures:

- Enabling the LGMP Server
- Configuring the LGMP Server
- Modifying the LGMP Server Display per VLAN
- Modifying LGMP Clients Per VLAN

Enabling the LGMP Server

You can enable the LGMP server using either the web agent or the CLI.

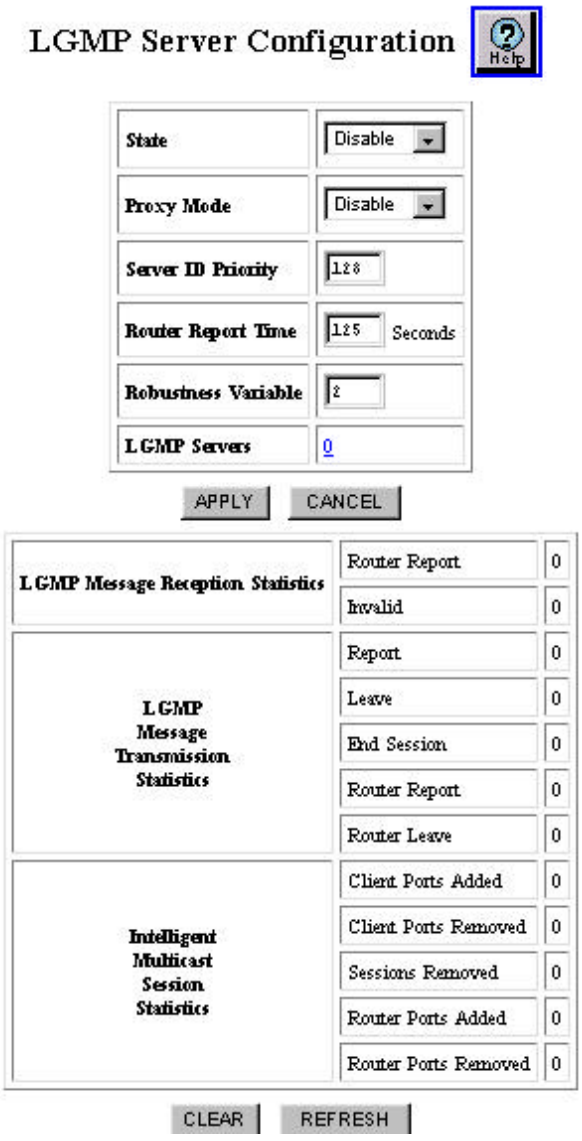
Enabling the LGMP Server Using the Web Agent

To enable the LGMP server using the web agent:

1. Select LGMP Snooping from the L2 > Intelligent Multicast group on the web agent window. The LGMP Server Configuration dialog box opens (Figure 16-9).

***Note:** You must enable intelligent multicasting on a global basis to activate the LGMP Server. LGMP serving is only active on VLANs with an IGMP interface enabled and IGMP snooping globally enabled.

Figure 16-10. LGMP Server Configuration Dialog Box



2. Select Enable from the State field, if it is not already displayed.

3. Click Apply to complete the operation or Cancel to ignore the operation.

Enabling the LGMP Server Using the CLI

To enable the LGMP server using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set lgmp server enable
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring the LGMP Server

You can configure the LGMP server using either the web agent or the CLI.

Configuring the LGMP Server Using the Web Agent

To configure the LGMP server using the web agent:

1. Select LGMP Snooping from the L2 > Intelligent Multicast group on the web agent window. The LGMP Server Configuration dialog box opens (Figure 16-9).

   ***Note:** You must enable intelligent multicasting on a global basis to activate the LGMP Server. LGMP serving is only active on VLANs with an IGMP interface enabled and IGMP snooping globally enabled.

2. Refer to Table 16-9 to configure the LGMP Server Configuration dialog box parameters:

Table 16-9. LGMP Server Configuration Dialog Box Parameters

Parameter	Definition
Enable State	Select to enable or disable LGMP server configuration. The default value is Disabled.
Proxy Mode	Select to enable or disable Proxy mode. Proxy mode allows the server to send LGMP router report and leave messages on behalf of neighbor routers on the same VLAN.

Table 16-9. LGMP Server Configuration Dialog Box Parameters
continued

Parameter	Definition
Server ID Priority	The priority of the LGMP server on this switch. The server ID priority and the IP address associated with the VLAN determine whether the LGMP server wins LGMP distribution election. The lower the number the more likely it will win the election. The valid range is 0 to 255. The default value is 128.
Router Report Time	The time interval (in seconds) between router reports sent by the LGMP server in distributor state. The valid range is 10 to 10,000. The default value is 125 seconds.
Robustness Variable	The scalar value used by non-distributor LGMP servers when timing out the LGMP server in the distributor state. The valid range is 2 to 10. The default value is 2.
LGMP Servers	Displays the number of LGMP servers and opens the LGMP Server Display per VLAN dialog box. **Note:** Only VLANs that have an active IGMP interface can be LGMP servers.
LGMP Message Reception Statistics	• **Router Report** - Displays the number of LGMP router report messages received. • **Invalid** - Displays the number of LGMP messages received with an invalid payload.

Table 16-9. LGMP Server Configuration Dialog Box Parameters
continued

Parameter	Definition
LGMP Message Transmission Statistics	• **Report** - Displays the number of LGMP report messages transmitted. • **Leave** - Displays the number of LGMP leave messages transmitted. • **End Session** - Displays the number of LGMP end session messages transmitted. • **Router Report** - Displays the number of LGMP router report messages transmitted. • **Router Leave** - Displays the number of LGMP router leave messages transmitted.
Intelligent Multicast Session Statistics	• **Client Ports Added**- Displays the number of add client events generated by LGMP. • **Client Ports Removed** - Displays the number of remove client events generated by LGMP. • **Sessions Removed**- Displays the number of remove session events generated by LGMP. • **Router Ports Added**- Displays the number of add router events generated by LGMP. • **Router Ports Removed**- Displays the number of remove router events generated by LGMP.

3. Click...

— APPLY to save your changes.

— CANCEL to restore previous settings.

— CLEAR to clear the statistics.

— REFRESH to refresh the contents of the table.

Configuring the LGMP Server Using the CLI

To configure the LGMP server using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set lgmp server <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying the LGMP Server Display per VLAN

You can modify the LGMP server display per VLAN using either the web agent or the CLI.

Modifying the LGMP Server Display per VLAN Using the Web Agent

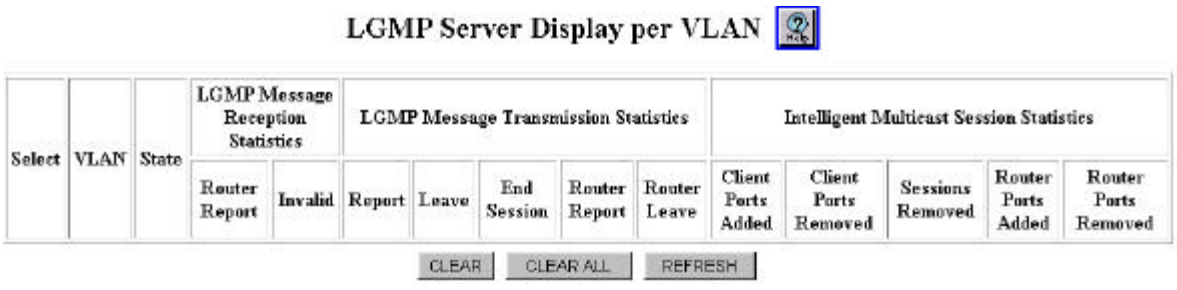
To modify the LGMP server display per VLAN using the web agent:

1. Select LGMP Snooping from the L2 > Intelligent Multicast group on the web agent window. The LGMP Server Configuration dialog box opens (see Figure 16-9).

   ***Note:** You must enable intelligent multicasting on a global basis to activate your LGMP server per VLAN configuration.

2. Select the number from the LGMP Servers column. The LGMP Server Display per VLAN dialog box opens (Figure 16-11).

Figure 16-11. LGMP Server per VLAN Dialog Box.



3. Refer to Table 16-10 to configure the LGMP Server Display per VLAN dialog box parameters:

Table 16-10. LGMP Server Display per VLAN Dialog Box Parameters

Parameter	Definition
Select	Select the LGMP server to modify.
VLAN	Displays the VLAN associated with the LGMP server.
State	Displays the current state of the LGMP server. • **Distributor** - The LGMP server serves LGMP messages to LGMP clients. • **Non-Distributor** - The LGMP server monitors the current distributor.
LGMP Message Reception Statistics	• **Router Report** - Displays the number of LGMP router report messages received per VLAN. • **Invalid** - Displays the number of LGMP messages received with an invalid payload per VLAN.

Table 16-10. LGMP Server Display per VLAN Dialog Box Parameters *continued*

Parameter	Definition
LGMP Messages Transmission Statistics	• **Report** - Displays the number of LGMP report messages transmitted per VLAN. • **Leave** - Displays the number of LGMP leave messages transmitted per VLAN. • **End Session** - Displays the number of LGMP end session messages transmitted per VLAN. • **Router Report** - Displays the number of LGMP router report messages transmitted per VLAN. • **Router Leave** - Displays the number of LGMP router leave messages transmitted per VLAN.
Intelligent Multicast Session Statistics	• **Client Ports Added**- Displays the number of add client events generated by LGMP per VLAN. • **Client Ports Removed**- Displays the number of remove client events generated by LGMP per VLAN. • **Sessions Removed**- Displays the number of remove session events generated by LGMP per VLAN. • **Router Ports Added**- Displays the number of add router events generated by LGMP per VLAN. • **Router Ports Removed**- Displays the number of remove router events generated by LGMP per VLAN.

4. Click...
   - — CLEAR to reset selected row information.
   - — CLEAR ALL to reset all statistics.
   - — REFRESH to view the latest information

Modifying the LGMP Server Display per VLAN Using the Web Agent

To modify the LGMP server display per VLAN using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set lgmp server <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Configuring/Viewing an LGMP Client

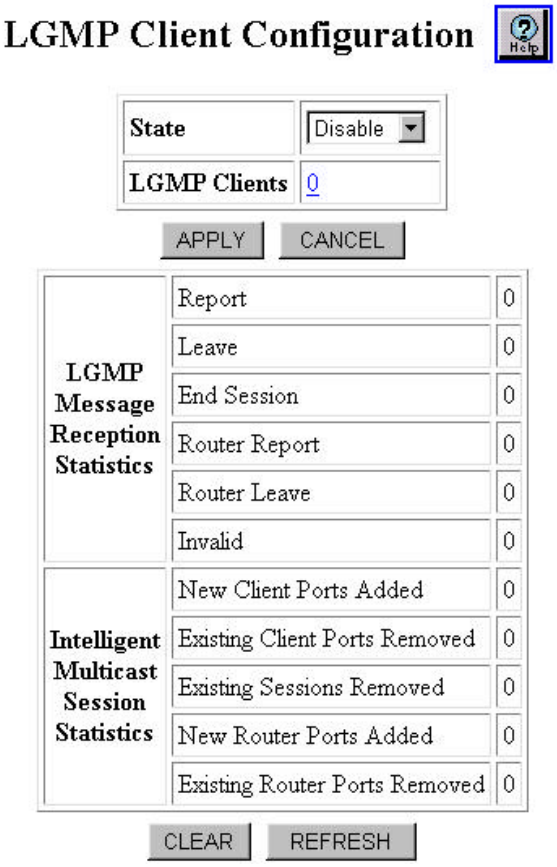
You can configure and view an LGMP client using either the web agent or the CLI.

Enabling/ Viewing an LGMP Client Using the Web Agent

To enable an LGMP client and view its statistics using the web agent:

1. Select LGMP Server from the L2 > Intelligent Multicast group on the web agent window. The LGMP Client Configuration dialog box opens (Figure 16-12).

Figure 16-12. LGMP Client Configuration Dialog Box



***Note:** You must enable intelligent multicasting on a global basis to activate LGMP client configuration.

2. Select Enable from the State field pull-down menu, if it is not already displayed.

3. Select Apply to complete the operation, or Cancel to ignore the operation.

4. Refer to Table 16-11 for an explanation of the LGMP Client Configuration dialog box parameters

Table 16-11. LGMP Client Configuration Dialog Box Parameters

Parameter	Definition
Enable State	Select to enable or disable LGMP client. The default value is Disabled.
LGMP Clients	Displays the number of LGMP clients per VLAN and opens the LGMP Client Displays per VLAN dialog box.
LGMP Message Reception Statistics	• **Report** - Displays the number of LGMP report messages received. • **Leave** - Displays the number of LGMP leave messages received. • **End Session** - Displays the number of LGMP end session messages received. • **Router Report** - Displays the number of LGMP router report messages received. • **Router Leave** - Displays the number of LGMP router leaves messages received. • **Invalid** - Displays the number of LGMP messages received with an invalid payload.
Intelligent Multicast Session Statistics	• **New Client Ports Added** - Displays the number of new clients added by LGMP. • **Existing Client Ports Removed** - Displays the number of clients removed by LGMP. • **Existing Sessions Removed** - Displays the number of sessions removed by LGMP. • **New Router Ports Added** - Displays the number of new routers added by LGMP. • **Existing Router Ports Removed** - Displays the number of new routers removed by LGMP.

5. Click CLEAR to clear the statistics, or REFRESH to refresh the contents of the table.

Enabling/ Viewing an LGMP Client Using the CLI

To enable an LGMP client using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set lgmp client enable
```

To view the LGMP client statistics using the CLI, enter the following command from User mode:

```
cajun# show lgmp client config
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Modifying LGMP Clients Per VLAN

You can modify LGMP client per VLAN using either the web agent or the CLI.

Modifying LGMP Clients Per VLAN Using the Web Agent

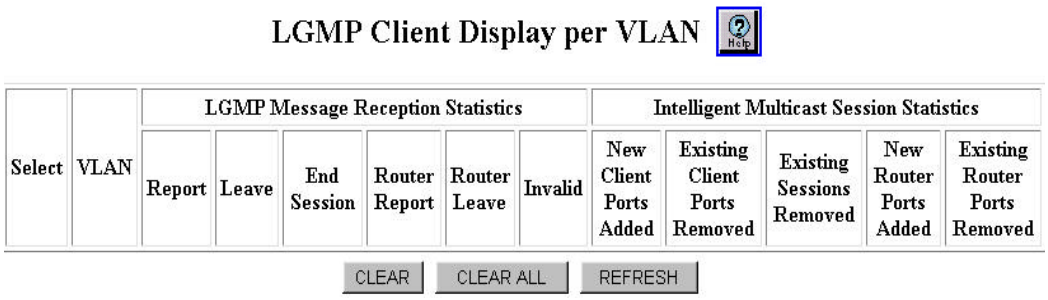
To modify LGMP clients per VLAN using the web agent:

1. Select LGMP Server from the L2 > Intelligent Multicast group on the web agent window. The LGMP Client Configuration dialog box opens (Figure 16-12).

   ***Note:** You must enable intelligent multicasting on a global basis to activate your LGMP client per VLAN configuration.

2. Select the number from the LGMP Clients field. The LGMP Client Display per VLAN dialog box opens (Figure 16-13).

Figure 16-13. LGMP Client Display per VLAN Dialog Box



3. Refer to Table 16-12 for an explanation of the LGMP Client Display per VLAN dialog box parameters.

Table 16-12. LGMP Client Display per VLAN Dialog Box Parameters

Parameter	Definition
Select	Select the LGMP client to modify.
VLAN	Displays the VLAN associated with the LGMP client.
LGMP Message Reception Statistics	• **Report** - Displays the number of LGMP report messages received per VLAN. • **Leave** - Displays the number of LGMP leave messages received per VLAN. • **End Session** - Displays the number of LGMP end session messages received per VLAN. • **Router Report** - Displays the number of LGMP router report messages received per VLAN. • **Router Leave** - Displays the number of LGMP router leaves messages received per VLAN. • **Invalid** - Displays the number of LGMP messages received with an invalid payload per VLAN.
Intelligent Multicast Session Statistics	• **New Client Ports Added** - Displays the number of new clients added by LGMP per VLAN. • **Existing Client Ports Removed** - Displays the number of clients removed by LGMP per VLAN. • **Existing Sessions Removed** - Displays the number of sessions removed by LGMP per VLAN. • **New Router Ports Added** - Displays the number of new routers added by LGMP per VLAN. • **Existing Router Ports Removed** - Displays the number of new routers removed by LGMP per VLAN.

4. Click...

   — CLEAR to reset selected row information.

   — CLEAR ALL to reset all statistics.

   — REFRESH to view the latest information.

Modifying LGMP Clients Per VLAN Using the CLI

To modify LGMP clients per VLAN using the CLI, enter the following command in Configure mode:

```
cajun(configure)# set lgmp client config <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Enabling/Viewing Cisco Group Management Protocol (CGMP) Snooping

You can enable CGMP snooping using either the web agent or the CLI.

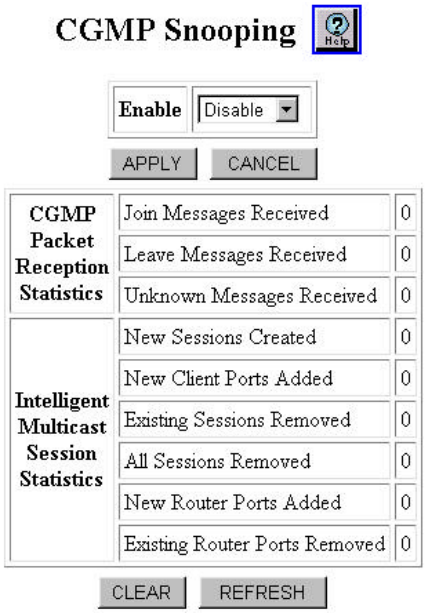
Enabling/ Viewing CGMP Snooping Using the Web Agent

To enable CGMP snooping and view its statistics using the web agent:

1. Select CGMP Snooping from the L2 > Intelligent Multicast group on the web agent window. The CGMP Snooping dialog box opens (Figure 16-14).

***Note:** You must enable intelligent multicasting on a global basis activate CGMP snooping configuration.

Figure 16-14. CGMP Snooping Dialog Box



2. Refer to Table 16-13 for an explanation of the CGMP Snooping dialog box parameters.

Table 16-13. CGMP Snooping Dialog Box Parameters

Parameter	Definition
Enable State	Select to enable or disable CGMP snooping.
CGMP Packet Reception Statistics	• **Join Messages Received** - Displays the number of CGMP join messages received. • **Leave Messages Received** - Displays the number of CGMP leave messages received. • **Unknown Messages Received** - Displays the number of unknown CGMP messages received.
Intelligent Multicast Session Statistics	• **New Sessions Created** - Displays the number of new multicast sessions created by CGMP snooping. • **New Client Ports Added** - Displays the number of new client ports added to a multicast session by CGMP snooping. • **Existing Sessions Removed** - Displays the number of existing multicast sessions that have been removed by CGMP snooping. • **All Sessions Removed** - Displays the number of times that all multicast sessions created by CGMP snooping were removed. • **New Router Ports Added** - Displays the number of new router ports added by CGMP snooping. • **Existing Router Ports Removed** - Displays the number of router ports that were created by the CGMP snooper and were removed by CGMP snooping.

3. Click ...
   - — APPLY to save your changes
   - — CANCEL to restore previous settings.
   - — CLEAR to clear the statistics
   - — REFRESH to refresh the contents of the table

Enabling/ Viewing CGMP Snooping Using the CLI

To enable CGMP snooping and view its statistics using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set cgmp en
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

17 Monitoring the Cajun Switch

Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- Interpreting Front Panel LED Displays
- Checking Active Alarms
- Using the Event Subsystem
- Click APPLY to save your changes, or CANCEL to restore previous settings.Setting Log Size

Interpreting Front Panel LED Displays

Refer to Table 17-1 fro an explanation of the Cajun P550/P880/P882 switch front-panel LEDs:

Table 17-1. Front Panel LED Display Interpretation

Module...	LED...	Behavior...	Indicates...
All Modules	Module Status	Solid green	Normal operation.
		Flashing yellow	Diagnostic failure.
		Off	Module not operational or not receiving power.
Gigabit Modules	TX and RX	Flashing yellow	Port sending/receiving traffic.
		Off	Port not sending/receiving traffic.

Table 17-1. Front Panel LED Display Interpretation *continued*

Module...	LED...	Behavior...	Indicates...
	Port	Solid green	Port enabled with link up.
		Flashing green	Port disabled with link up.
		Flashing yellow	Hardware failure.
		Off	No link.
	HD/FD	Solid green	Full-duplex operation negotiated.
		Flashing yellow	Hardware failure.
		Off	No link.
10/100 Modules	Port	Solid green, with yellow flash	Port enabled and sending and receiving traffic Traffic indicated by yellow flashes.
		Flashing green	Port disabled with link up.
		Flashing yellow	Hardware failure.
		Off	No link.

Checking Temperature Status and Configuring Thresholds

You can check the temperature status and configuring thresholds using either the web agent or the CLI.

Checking Temperature Status and Configuring Thresholds

You can check the temperature status and configure thresholds using either the web agent or the CLI.

Checking Temperature Status and Configuring Thresholds Using the Web Agent

To check the temperature status and configure thresholds from the web agent:

1. Select Temperature system from the System > Configuration group on the web agent windows. The Temperature System dialog box for Layer 2 (Figure 17-1) or Layer 3 (Figure 17-2) opens.

Figure 17-1. Temperature System Dialog Box (Layer 2)

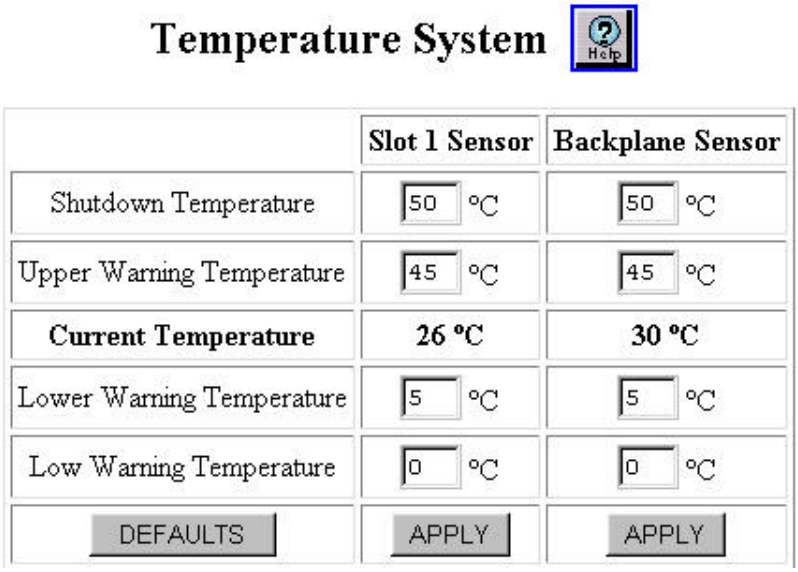
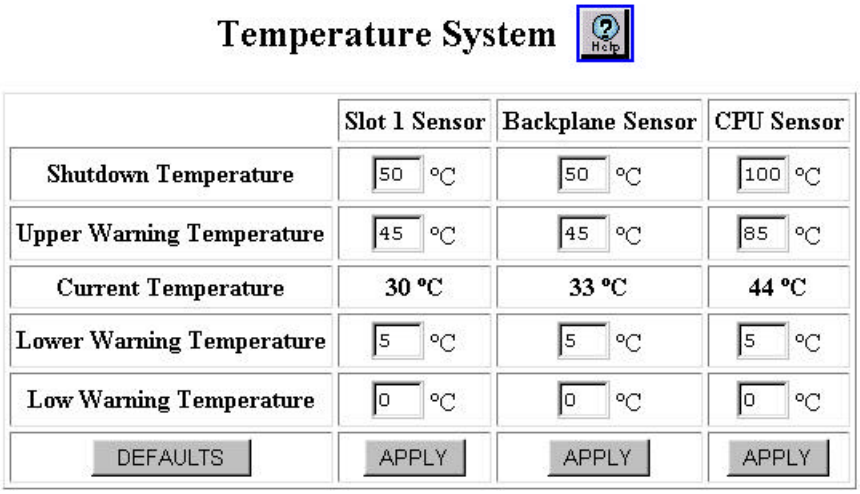


Figure 17-2. Temperature System Dialog Box (Layer 3)



2. Refer to Table 17-2 to set the threshold values:

Table 17-2. Temperature Threshold Values

Threshold	Defines...
Shutdown Temperature (Layer 2)/ Warning Temperature (layer 3)	Value in degrees Celsius that causes the switch to send a trap to the network management station and triggers a shutdown for a layer 2 CPU sensor and a warning temperature message for a multilayer CPU sensor when it is passed. The layer 2 default value is 50 degrees Celsius, and the multilayer CPU sensor is 100 degrees Celsius.
Upper Warning Temperature	Value in degrees Celsius that causes the switch to send a high temperature threshold warning when it is passed. The layer 2 default value is 45 degrees Celsius, and the layer 3 CPU sensor is 85 degrees Celsius.
Lower Warning Temperature	Value that in degrees Celsius that when passed causes the switch to send a warning that the temperature is approaching the low temperature threshold. By default, this value is 5 degrees Celsius.
Low Shutdown Temperature (Layer 2)/Low Warning Temperature (Layer 3)	Indicates the low shutdown temperature for a switch to reset the warning and high thresholds. This value prevents the switch from sending traps continually if the temperature is hovering around the threshold value. The default value is 0 degrees Celsius.

Checking Temperature Status and Configuring Thresholds Using the CLI

To check the temperature status using the CLI, enter the following command from User mode:

```
cajun# show temperature
```

To configure temperature threshold values using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set temperature <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Checking Active Alarms

Each switch stores a table of active alarms from which you can view a list of open issues without having to view the entire event log. This provides you with a quick snapshot of the switch's health.

This section provides the following procedures:

- Viewing the Active Alarm Table
- Using the Event Subsystem
- Configuring the Protocol Event Log
- Viewing the Event and Shutdown Logs
- Viewing Event Statistics

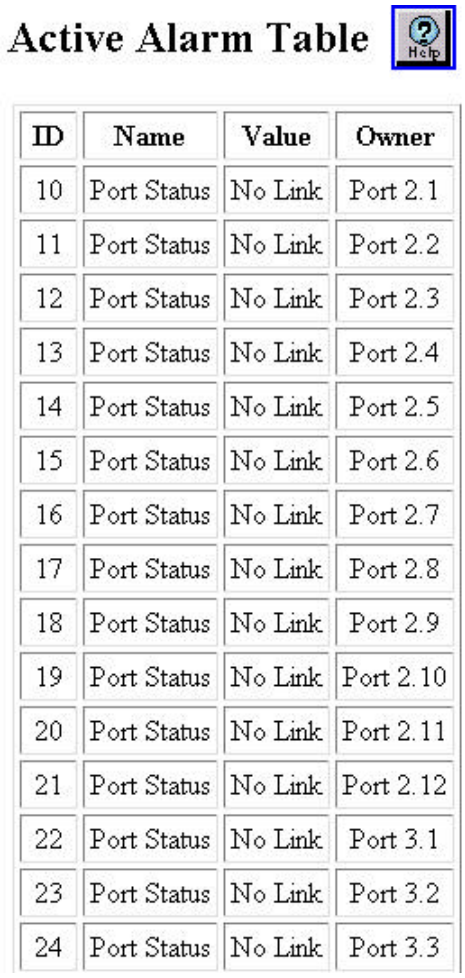
Viewing the Active Alarm Table

You can view the active alarm table using either the web agent or the CLI.

Viewing the Active Alarm Table Using the Web Agent

To view the Active Alarm table, select Active Alarms from the Events group on the Web Agent window. The Active Alarm Table opens (Figure 17-3).

Figure 17-3. Active Alarm Table Dialog Box



Active Alarm Table

ID	Name	Value	Owner
10	Port Status	No Link	Port 2.1
11	Port Status	No Link	Port 2.2
12	Port Status	No Link	Port 2.3
13	Port Status	No Link	Port 2.4
14	Port Status	No Link	Port 2.5
15	Port Status	No Link	Port 2.6
16	Port Status	No Link	Port 2.7
17	Port Status	No Link	Port 2.8
18	Port Status	No Link	Port 2.9
19	Port Status	No Link	Port 2.10
20	Port Status	No Link	Port 2.11
21	Port Status	No Link	Port 2.12
22	Port Status	No Link	Port 3.1
23	Port Status	No Link	Port 3.2
24	Port Status	No Link	Port 3.3

Viewing the Active Alarm Table Using the CLI

To view the Active Alarm table using the CLI, enter the following command from User mode:

```
cajun# show alarms
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Using the Event Subsystem

There are two switch system activity logs for layer 3:

- **Event Log** - stores a large table of events. The size of the table is user-settable. Because these events are stored in switch memory, the list is cleared each time the switch reboots.
- **Shutdown Log** - stores the same information as the Event Log, but generally in a smaller table because the table is stored in the switch's nonvolatile RAM (NVRAM). This log list is particularly useful in assessing the cause of a switch failure, because the information is retained even after the switch restarts.

Configuring the Protocol Event Log

You can use the protocol event log to enable RIP and OSPF packet tracing for layer 3 only. RIP requests and responses received and sent through all RIP interfaces are logged to the event log as protocol events. OSPF packet types received and sent through all OSPF interfaces are logged to the event log as protocol events. AppleTalk packet types received and sent through all AppleTalk interfaces are logged to the event log as protocol events. LDAP packet types received and sent through all LDAP interfaces are logged to the event log as protocol events.

*** Note:** Enabling the protocol event log may cause the event log to be rapidly filled with protocol events.

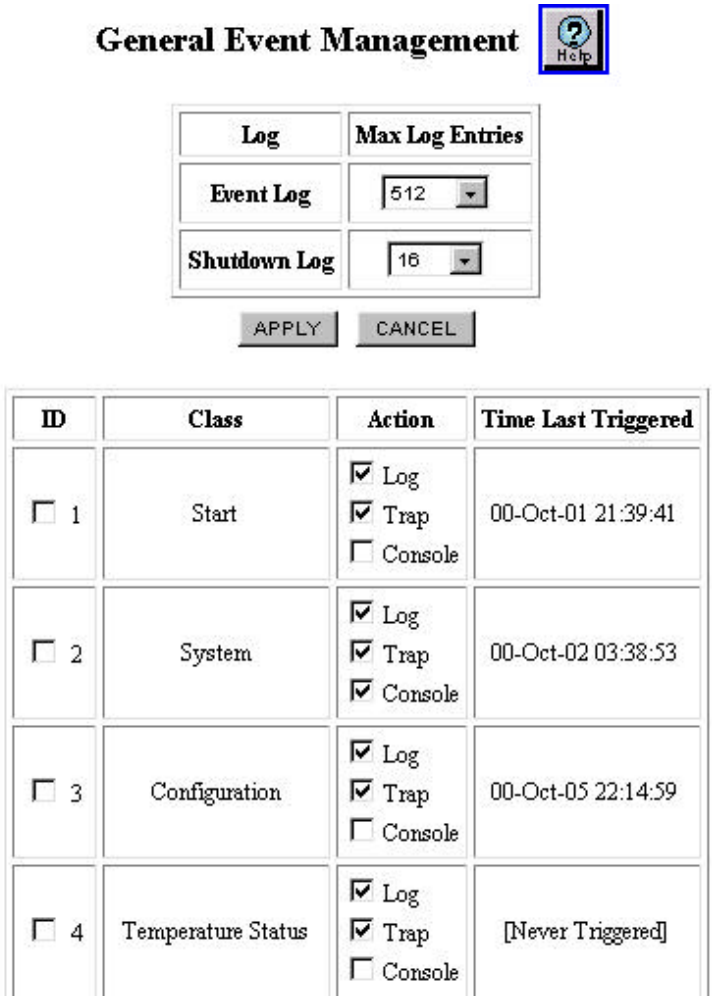
You can configure the protocol event log using either the web agent or the CLI.

Configuring the Protocol Event Log Using the Web Agent

To configure the protocol event log using the web agent:

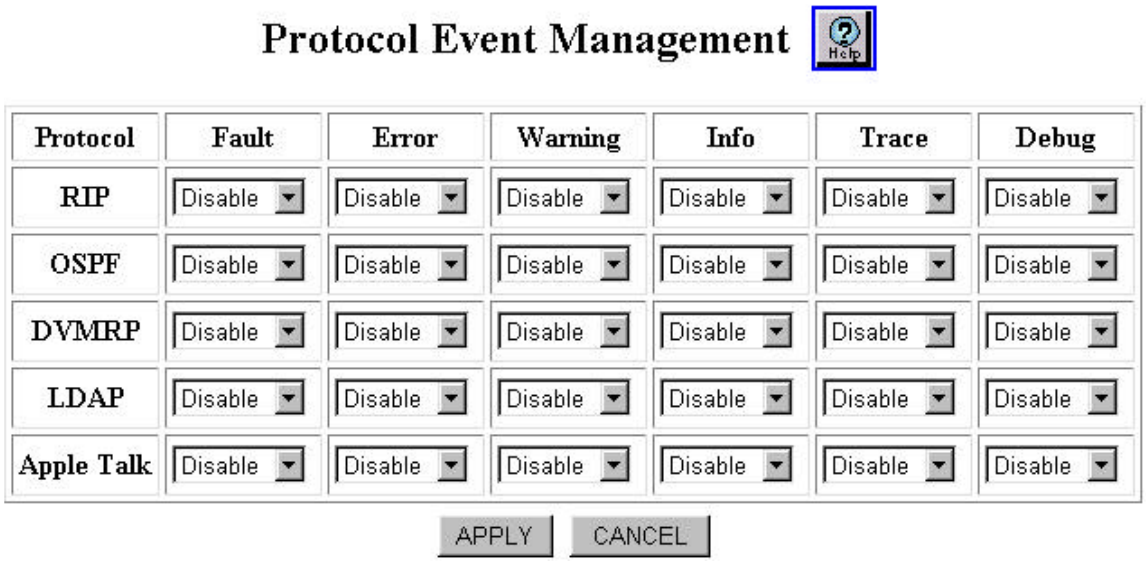
1. Select **General Events** from the **Events** group on the web agent window. The **General Event Management** dialog box opens (Figure 17-4).

Figure 17-4. General Event Management Dialog Box (Partial View)



2. Select one of the following from the **ID** column:
   - RIP
   - OSPF
   - LDAP
   - AppleTalk
3. Click APPLY to save your changes, or CANCEL to restore previous settings.
4. Select Protocol Events from the Events group on the web page window. The Protocol Event Management dialog box opens (Figure 17-5).

Figure 17-5. Protocol Event Management Dialog Box



5. Refer to Table 17-3 to configure the Protocol Event Management dialog box parameters for the specific protocols that you have configured on your switch:

Table 17-3. Protocol Event Management Dialog Box Parameters

Column Heading	Parameter
Fault	Select **Enable** to display serious errors that can cause a system crash, for example, panic. The default is **Disable**.
Error	Select **Enable** to display serious errors that will not cause a system crash but can contribute protocol problems.
Warning	Select **Enable** to display non-critical errors. The default is **Disable**.
Info	Select **Enable** to display Event details. The default is **Disable.**
Trace	Select **Enable** to display RIP and OSPF packet tracing. The default is **Disable**.
Debug	Select **Enable** to display event messages used to troubleshoot a network problem. The default is **Disable**.

6. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring the Protocol Event Log Using the CLI

To configure the protocol event log using the CLI, enter the following command from Configure mode:

```
cajun(configure)# logging protocol event
<protocol>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing the Event and Shutdown Logs

You can view the Event and Shutdown logs using either the web agent or the CLI.

Viewing the Event and Shutdown Logs Using the Web Agent

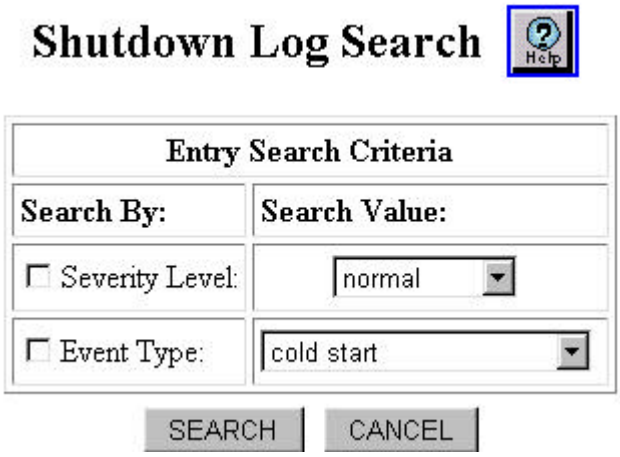
To view the Event and Shutdown logs using the web agent:

1. Select either Event Log or Shutdown Log from the Events group on the web agent window. The Event Log Search dialog box (Figure 17-6) or the Shutdown Log Search dialog box opens (Figure 17-7).

Figure 17-6. Event Log Search Dialog Box

Figure 17-7. Shutdown Log Search Dialog Box

2. Click the Severity Level checkbox in the Search By: column on either dialog box.



3. Select the severity level to filter on a particular severity level for events from the Severity Level field pull-down menu from either dialog box.

4. Select an event to filter on a particular event type from the Event Type field pull-down menu from either dialog box. The event log entries open in the Event Log window (Figure 17-8).

Figure 17-8. Event Log Dialog Box

5. Refer to Table 17-4 for a explanation Event Log window parameters:

Table 17-4. Event Log Window Parameters

Entry	Definition
Log ID	Displays the number of this event in the log FIFO (First In First Out).
Event ID	Displays an index that identifies the event class.
Time Stamp	Displays the date and time the event was recorded.

Table 17-4. Event Log Window Parameters continued

Entry	Definition
Severity	Displays the severity of the event. The possibilities are: • Informative • Warning • Error • Severe Error • Failure
Type	Displays a description of the event type (for example System start and Status Change).
Description	Displays a text string that describes the specific event.

6. Click ...

   — SEARCH to view the event or shutdown logs from either dialog box.

   — CANCEL to restore previous settings.

   — CLEAR EVENT LOG to clear the event log settings.

   ***Note:** You can clear the event log by clicking Clear Event Log, If you have write-access. This option is not available if you do not have write-access.

Viewing the Event and Shutdown Logs Using the CLI

To view the Event and Shutdown logs using the CLI, enter the following command from User mode:

```
cajun show logging <num-events|shutdown>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Viewing Event Statistics

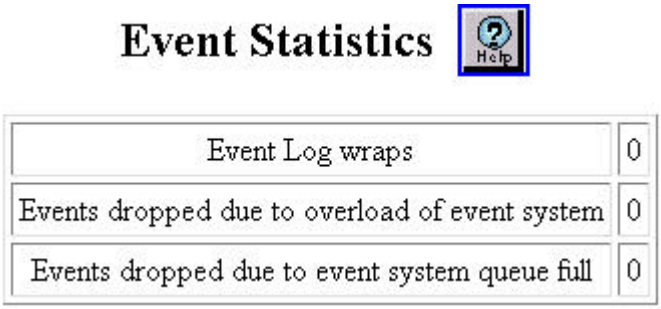
You can view event statistics using either the web agent or the CLI.

Viewing Event Statistics Using the Web Agent

To view event statistics using the web agent:

1. Select Event Statistics from the Events group on the web agent window. The Event Statistics dialog box opens (Figure 17-9).

Figure 17-9. Event Statistics Dialog Box



2. Refer to the Table 17-5 for an explanation on the **Event Statistics** window parameters.

Table 17-5. Event Statistics Window Parameters

Parameter	Definition
Event Log wraps	Displays the number of times the Event Log has wrapped. The Event Log may or may not wrap, depending on how many events have been sent to the Event Log and when it was last cleared. When the event log does wrap, the old events are discarded and replaced with the newest events.
Events dropped due to overload of event system	Displays the number of events that were dropped to prevent overloading.
Events dropped due to event system queue full	Displays the number of events that were dropped due to a full Event System queue.

Viewing Event Statistics Using the CLI

To view event statistics using the CLI, enter the following command from User mode:

```
cajun show logging <num-events>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Setting Log Size

You can set the log size using either the web agent or the CLI.

Setting Log Size Using the Web Agent

To set the log size using the web agent:

1. Select General Events from the Events group on the web agent window. The General Event Management dialog box opens (Figure 17-4).
2. Select the number of entries you want to store in each of the switch event logs from the Event Log field pull-down menu.
3. Refer to Table 17-6 for an explanation of the Event Log and Shutdown Log parameters on the General Event Management dialog box:

Table 17-6. Event Log and Shutdown Log Fields Parameters

Log	Purpose
Event Log	A detailed, ongoing record of syslog messages that are stored in the router's history table. This log is stored in memory and is erased if the system shuts down or reboots.
Shutdown Log	Contains a list of events that occurred before the last time the switch was shutdown. Because this log is stored in nonvolatile memory, it is preserved during a switch reboot or shutdown. It is designed to help you analyze the events that occurred immediately prior to a switch shutdown or reset.

4. Refer to Table 17-7 for an explanation of the items listed in the Class column on the General Event Management dialog box:

Table 17-7. Class Column Items

Class	Determines whether or not the switch sends a notification...
Start	Upon system start.
System	For system events.
Configuration	For each configuration change (for example, enabling and disabling ports).
Temperature Status	Of temperature status changes. Temperature status message could precede a switch shutdown, and are often critical.
Resource	Upon a change in system resources.
Fan Status	Of fan status. Fan failures will eventually lead to overheating the system. Fan Status message provide a good early warning for a failure that could eventually cause the switch to shut down.
Service Port Status/ User Port Status	Of Port status changes for service and user ports. Set a port as either service port/user port from the port configuration page. The purpose of this feature is to allow you to use different notification level for critical (service ports), if desired.
Authentication Failure	When the switch detects an authentication failure. This is a security-related feature used to detect unauthorized SNMP activity.
Bridge Status	Of changes in bridge status.
Switch Fabric	Of failures in the switch fabric. These are critical failures and should be monitored closely.
OSPF	For OSPF events if OSPF protocol event logging is enabled.
RIP	For RIP events if RIP protocol event logging is enabled.
LDAP	For LDAP events if LDAP protocol event logging is enabled.
AppleTalk	For AppleTalk events if AppleTalk protocol event logging is enabled.

5. Click APPLY to save your changes, or CANCEL to restore previous settings.

Setting Log Size Using the CLI

To set log size using the CLI, enter the following command from User mode:

```
cajun#show logging history size <128, 512, 1024,
2048>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Configuring Event Notification

You can configure event notification using either the web agent or the CLI.

Configuring Event Notification Using the Web Agent

To configure event notification:

1. Select Event Log from the Events group on the web agent window. The Event Log Search dialog box opens (Figure 17-6).
2. Click the check box next to the Event Type field.
3. Select an event type from the pull-down menu. The delivery of event information is enabled when this type of event occurs.
4. Refer to Table 17-8 for an explanation of the parameters in the Action column on the General Event Management dialog box. If you do not select an event, no action is taken when an event of this event class occurs.

Table 17-8. Action Column Parameters

Setting...	Determines...
Log	Event entry entered in event and shutdown logs.
Trap	SNMP trap message (event notification) sent to designated trap receivers.
Console	Displays the event information to the console serial port connected at the switch front panel.

5. Click APPLY to save your changes, or CANCEL to restore previous settings.

Configuring Event Notification Using the CLI

To configure event notification using the CLI, enter the following command from Configure mode:

```
cajun(configure)# logging history <options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

18 Monitoring and Configuring the Forwarding Cache

Overview

The information and procedures provided in this chapter pertain to layer 3 module configuration only:

- Configuring the Fowarding Cache
- Displaying Frame Fowarding Statistics
- Searching the Routing Cache for an Entry
- Displaying the Forwarding Cache

Configuring the Fowarding Cache

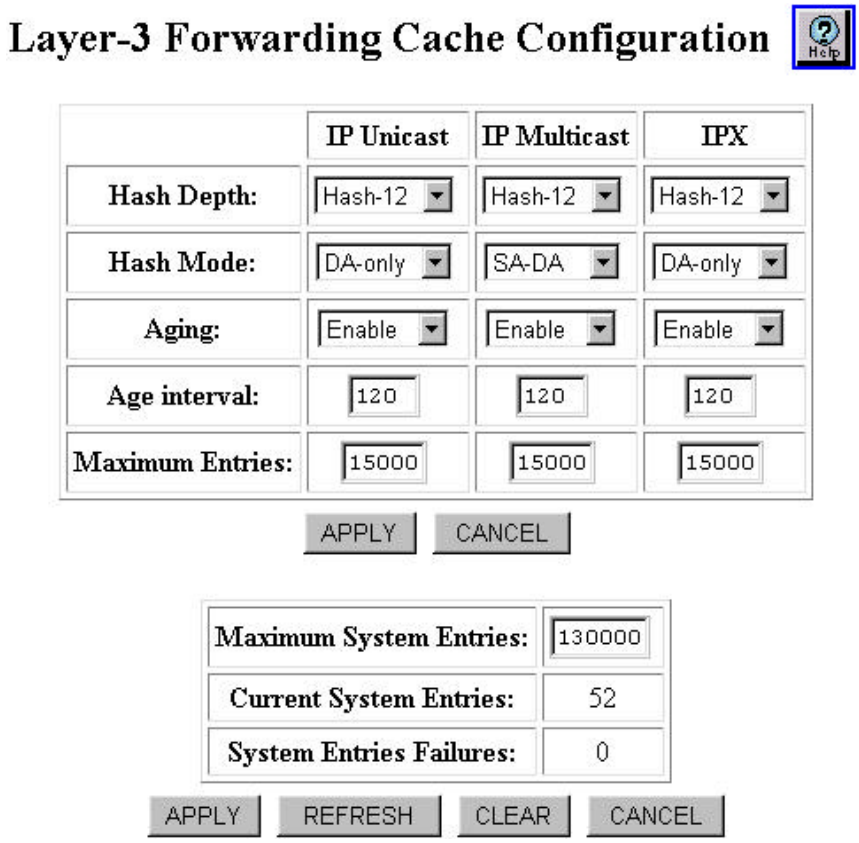
The forwarding cache enables you to configure the multilayer media module's forwarding tables. You can configure the forwarding cache using the web agent or the CLI.

Configuring the Forwarding Cache Using the Web Agent

To configure the forwarding cache using the web agent:

1. Select Cache Configuration from the Routing > L3 Forwarding Cache group on the web agent window. The Layer 3 Forwarding Cache Configuration dialog box opens (Figure 18-1).

Figure 18-1. Layer-3 Forwarding Cache Configuration Dialog Box



2. Configure the tree configuration parameters. Refer to Table 18-1 for an explanation of the Layer-3 Fowarding Cache Configuration dialog box parameters for tree configuration:

Table 18-1. Layer-3 Forwarding Cache Configuration Dialog Box Parameters for Tree Configuration

Tree Configuration		
Field...	**For the protocol...**	**Allows you to...**
Hash Depth	IP Unicast IP Multicast IPX	Configure the hash depth for the IP unicast, IP multicast, and IPX protocols. The options are: • **Hash-8** - An 8-bit memory bucket used to store information about the source or destination protocol address (or both). • **Hash -10** - A 10-bit memory bucket used to store information about the source or destination protocol address (or both). • **Hash-12** - A 12-bit memory bucket used to store information about the source or destination protocol address (or both).
Hash Mode	IP Unicast IP Multicast IPX	Configure the table hash lookup mode for the IP unicast, IP multicast and IPX protocols. The options are: • **DA-only** - Forwarding entries input to the forwarding table are limited to using protocol destination address only. • **SA-DA** - Forwarding entries input to the forwarding table are limited to using destination and source address only.
Aging	IP Unicast IP Multicast IPX	Configure the IP unicast, IP multicast, or IPX protocols forwarding table entry aging status as either **Enable (default)** or **Disable**.

***Table 18-1. Layer-3 Forwarding Cache Configuration Dialog Box Parameters for Tree Configuration** Continued*

Tree Configuration *Continued*		
Field...	**For the protocol...**	**Allows you to...**
Age Interval	IP Unicast IP Multicast IPX	The IP unicast, IP multicast, or IPX protocols forwarding table entry aging period (in seconds). The default value is **120 seconds**.
Maximum Entries	IP Unicast IP Multicast IPX	The number of active entries in the IP unicast, IP multicast, or IPX protocol forwarding table. This is the maximum number of active entries per fabric port. Additional flows are forwarded by the supervisor module. The default value is **15000**.

3. Click ...
   - APPLY to save your changes
   - CANCEL to restore previous settings
   - REFRESH to update your system configuration
   - CLEAR to reset all configuration parameters to zero.

Configuring the Fowarding Cache Using the CLI

To configure the forwarding cache using the CLI, enter the following command from Configure mode:

```
cajun(configure)# ip multicast route-cache
<options>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Monitoring the Forwarding Cache Statistics

Monitoring the forwarding cache statistics includes:

- Displaying Frame Fowarding Statistics
- Searching the Routing Cache for an Entry

Displaying Frame Fowarding Statistics

The frame forwarding statistics indicate the performance of each of the multilayer media modules in respect to layer 3 routing and forwarding. You can display the frame forwarding statistics from either the web agent or the CLI.

Displaying Frame Fowarding Statistics Using the Web Agent

To display the frame forwarding statistics using the web agent:

1. Select Forwarding Statistics from the Routing > L3 Forwarding Cache group on the web agent window. The Frame Forwarding Statistics dialog box opens (Figure 18-2).

Figure 18-2. Frame Forwarding Statistics Dialog Box

Frame Forwarding Statistics Help

Select	FIRE Fabric Port	L3 Total	L3 Frame Cache Hits	Percent Cache Hits	L3 Slow Path Frames	Percent Slow Path	L3 Drop Frames	Percent Drops	RX Frame Count (T2)	L2 Frame Count (T2)
☐	1	74	0	0%	74	100%	0	0%	298,693	0
☐	2	36	0	0%	36	100%	0	0%	96	96
☐	4	30	0	0%	30	100%	0	0%	80	80
☐	6	109,711	109,476	99%	235	0%	0	0%	110,754	1,059
☐	7	6	0	0%	6	100%	0	0%	11	11

CLEAR REFRESH

2. Refer to Table 18-2 for an explanation for the Frame Forwarding Statistics dialog box parameters:

Table 18-2. Frame Forwarding Statistics Dialog Box Parameters

Parameter	Defines the...
FIRE Fabric Port	Fabric port associated with the layer 3 module. The switch has 13 fabric ports. The supervisor module slot uses one fabric port: the media module slots each use two fabric ports. The supervisor module slot uses fabric port 1, the first media module slot uses fabric ports 2 and 3, and so on.
L3 Total (T2)	Total number of frames received on the fabric port.
L3 Frame Cache Hits	Number of packets received on the fabric port that were successfully matched against existing forwarding entries in the layer 3 (L3) address cache.
Percent Cache Hits	Total percentage of successful matches between packets received on a fabric port and the percent of those packets that matched the layer 3 address cache entries.
L3 Slow Path Frames	Number of frames received on a fabric port that were *not* successfully matched against existing forwarding entries in the layer 3 (L3) address cache. Subsequently, these frames were forwarded to the supervisor module (slow path). All frames sent to the supervisor module are routed in software.
Percent Slow Path	Total percentage of unsuccessful matches between packets received on a fabric port and the percent of those packets that did not match the layer 3 address cache entries.
L3 Drop Frames	Number of layer 3 frames that were dropped because they did not match the layer 3 address cache entries.
Percent Drops	Total percent of layer 3 frames dropped.
RX Frame Count (T2)	Total number of frames received on a fabric port.
L2 Frame Count (T2)	Number of layer 2 frames received on a fabric port that were forwarded on to an associated VLAN.

Displaying Frame Fowarding Statistics Using the CLI

To display the frame forwarding statistics using the CLI, enter the following commands from Configure mode:

```
Cajun(configure)# show ip dvmrp forwarding
cache
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Searching the Routing Cache for an Entry

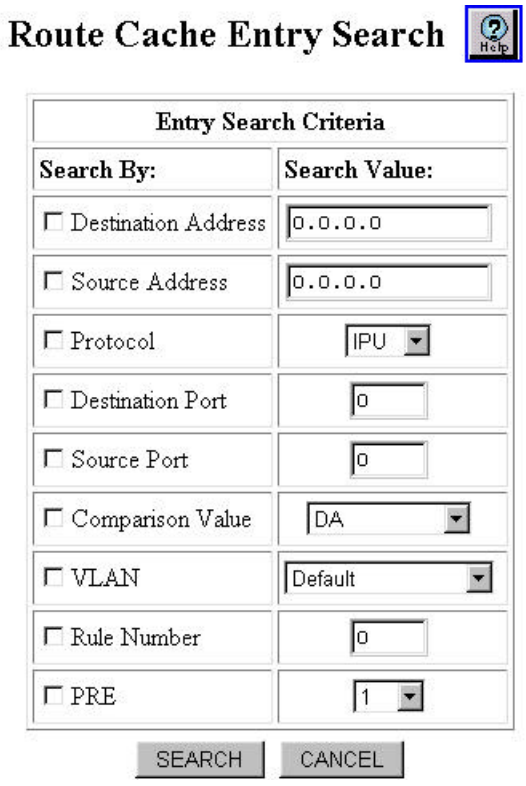
You can search the routing cache for an entry using either the web agent or the CLI.

Searching the Routing Cache for an Entry Using the Web Agent

To search the L3 address cache using the web agent:

1. Select Entry Search from the Routing > L3 Forwarding Cache group on the web agent window. The Route Cache Entry Search dialog box opens (Figure 18-3).

Figure 18-3. Route Cache Entry Search Dialog Box



2. Select the search criteria that you want to use to find more specific information on available routes from the Search By column.
   For example, if you want to find all entries in the routing cache that contain a VLAN entry, you would select VLAN from the Search By column, and select the appropriate vlan from the pull-down menu.

   Refer to Table 18-3 for an explanation of the Route Cache Entry Search dialog box parameters:

Table 18-3. Route Cache Entry Search Dialog Box Parameters

Parameter	Allows you to search for all entries...
Destination Address	Within the routing cache that match the specified destination address (IP address).
Source Address	Within the routing cache that match the specified source address (IP address).
Protocol	By protocol identifier. By default, this field is 0 for IP (for example, not supported by IP).
Destination Port	Within the routing cache that match the specified destination port (IPU, IPM, IPX).
Source Port	Within the routing cache that match the specified source port (IPU, IPM, IPX).
Comparison Value	Within the routing cache that match the specified comparison value (TCP/UDP). Values include: • **DA** - Destination address • **DASA** - Destination and source address • **DAPROT** - Destination address and protocol • **DADP** - Destination address and destination port number • **DASAPROT** - Destination and source address and protocol • **DASADPSP** - Destination and source address, and the corresponding destination and source port numbers
VLAN	Within the routing cache that match the VLANs listed in the pull-down menu.

Table 18-3. Route Cache Entry Search Dialog Box Parameters
Continued

Parameter	Allows you to search for all entries...
Rule Number	Within the routing cache that matches the specified rule number associated with an access list.
PRE	That match the PRE that is associated with the fabric port ID.

Searching the Routing Cache for an Entry Using the CLI

To search the L3 address cache using the CLI, enter one of the following commands from **Priv** mode for the specific routing cache:

```
cajun># show ip unicast cache

cajun># show ip multicast cache

cajun># show ipx cache
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

Displaying the Forwarding Cache

You can display the Forwarding cache information using either the web agent or the CLI.

Displaying the Forwarding Cache Using the Web Agent

To display the forwarding cache information using the web agent:

1. Select Cache Contents from the Routing > L3 Forwarding Cache group on the web agent window. The FE Cache dialog box opens (Figure 18-4).

Figure 18-4. FE Cache Dialog Box

FE Cache Help

Select	PRE	Type	Mode	Memory Use in Bytes	Total Entries	Current Entries	Aged Entries	Duplicate Add Attempts	Failed Add Attempts	Entries Removed due to Route Deletes	Entries Removed due to Route Changes	Lookup Hits	Lookup Misses	Lookup Levels
☐	1	IP_UNI	DA-Only	456	13	4	0	0	0	0	0	9	10	4
☐	1	IP_MUL	SA-DA	0	0	0	0	0	0	0	0	0	0	0
☐	1	IPX	DA-Only	0	0	0	0	0	0	0	0	0	0	0
☐	6	IP_UNI	DA-Only	912	14198	8	14157	37	0	24	0	9	10	5
☐	6	IP_MUL	SA-DA	0	0	0	0	0	0	0	0	0	0	0
☐	6	IPX	DA-Only	0	0	0	0	0	0	0	0	0	0	0

Clear | Refresh | Flush Entry | Flush Table

2. To modify your FE Cache table, do one of the following:
   - Select the entry and click Flush Entry to delete one or more entries
   - Click Flush Table to clear the entire table
   - Click REFRESH to refresh the contents of the table
   - Click Clear to remove the statistics only (the entry in the table remains).

3. Refer to Table 18-4 for an explanation of the FE Cache dialog box fields:

Table 18-4. FE Cache Dialog Box Fields

Parameter	Defines...
PRE	The Packet Routing Engine in question.
Type	The type of packet (for example, IP unicast, IP multicast).
Mode	The table mode which includes: • DA-Only • SA & DA • SA only The table mode indicates what values are used in a comparison to determine whether or not a packet is forwarded.
Memory Use in Bytes	Memory used by each entry.
Total Entries	The number of cumulative entries since the last time the statistics were cleared.
Current Entries	The number of active entries.
Aged Entries	The number of entries aged out.
Duplicate Add Attempts	The number of attempts at adding some slow path entries.
Failed Add Attempts	The number of failed attempts at adding a forwarding entry.
Entries Removed Due to Route Deletes	The number of entries removed because of route deletions.
Entries Removed Due to Route Changes	The number of entries removed because of route changes.
Lookup Hits	Cache hits.
Lookup Misses	Cache misses.
Lookup Levels	Cache depth.

Displaying the Forwarding Cache Using the CLI

To display the forwarding cache information using the CLI, enter one of the following commands from Priv mode for the specific routing cache:

```
cajun># show ip unicast cache

cajun># show ip multicast cache

cajun># show ipx cache
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about these commands.

19 Analyzing Network Performance Using RMON and Ethernet Statistics

Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- Viewing Network Statistics
- Setting Up a Mirror Port

Viewing Network Statistics

You can view a variety of statistics from the switch interface that allows you to monitor network performance and troubleshoot network problems.

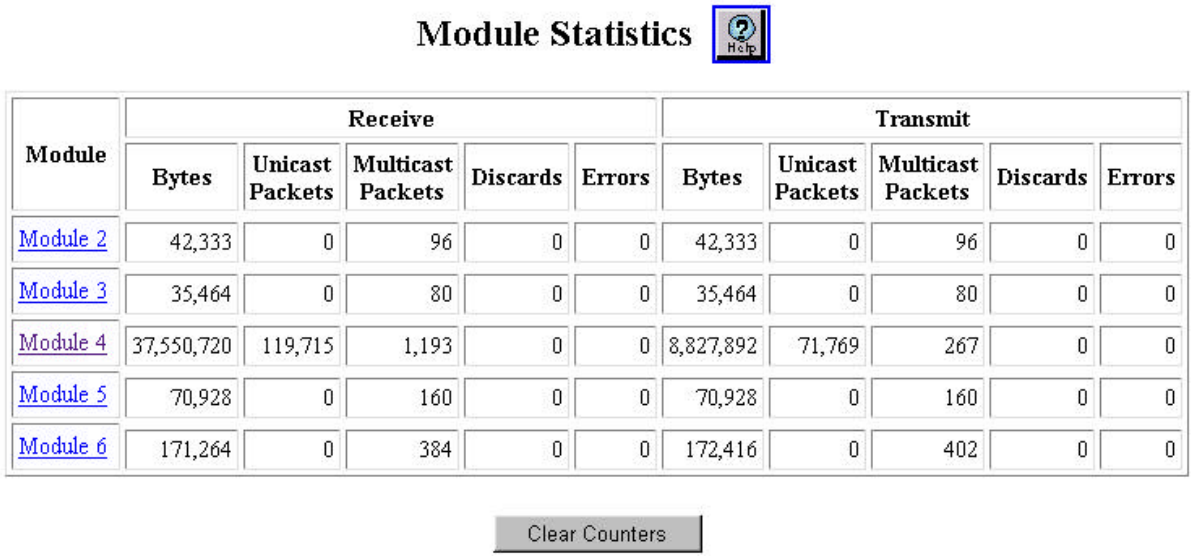
You can view statistics using either the web agent or the CLI.

Viewing Network Statistics Using the Web Agent

To view network statistics using the web agent:

1. Select Statistics from the Modules and Ports group on the web agent window. The Module Statistics dialog box opens (Figure 19-1).

Figure 19-1. Module Statistics Dialog Box



Module Statistics

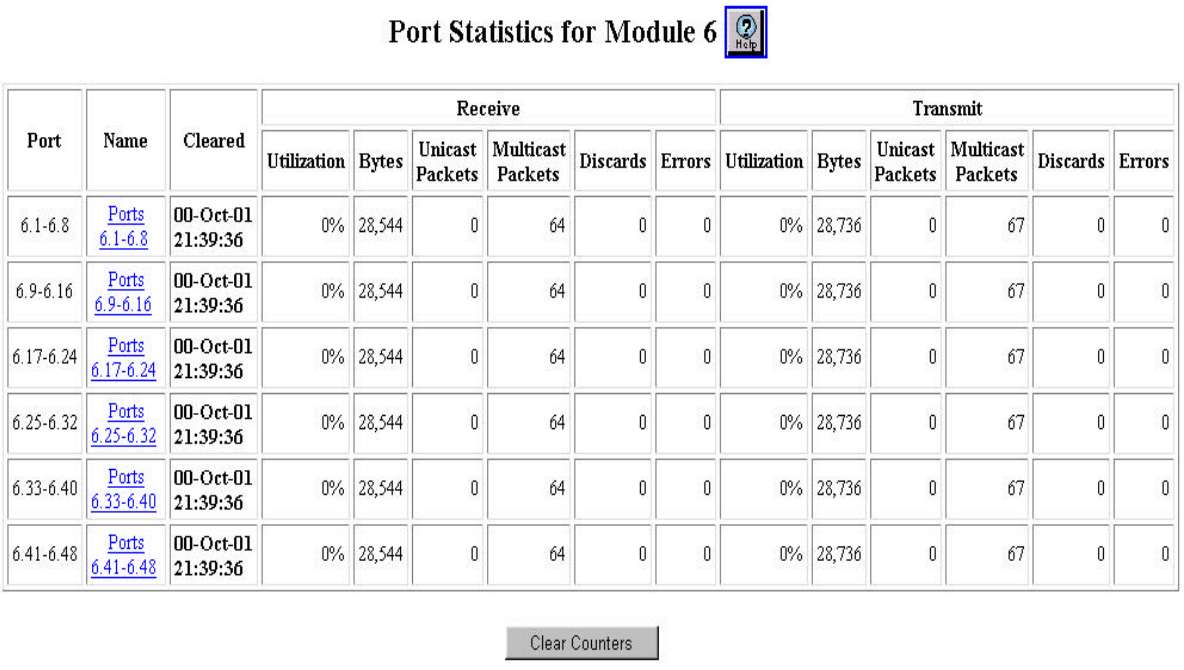
Module	Receive					Transmit				
	Bytes	Unicast Packets	Multicast Packets	Discards	Errors	Bytes	Unicast Packets	Multicast Packets	Discards	Errors
Module 2	42,333	0	96	0	0	42,333	0	96	0	0
Module 3	35,464	0	80	0	0	35,464	0	80	0	0
Module 4	37,550,720	119,715	1,193	0	0	8,827,892	71,769	267	0	0
Module 5	70,928	0	160	0	0	70,928	0	160	0	0
Module 6	171,264	0	384	0	0	172,416	0	402	0	0

Clear Counters

2. Select Clear Counters to get a fresh view of the statistics being gathered. This resets all of the counters to zero, so that you can track the counters from a specific point forward.

3. Select a module from the Module column to view statistics for that specific module. The Port Statistics dialog box opens (Figure 19-2).

Figure 19-2. Port Statistics Dialog Box



Port Statistics for Module 6

Port	Name	Cleared	Receive						Transmit					
			Utilization	Bytes	Unicast Packets	Multicast Packets	Discards	Errors	Utilization	Bytes	Unicast Packets	Multicast Packets	Discards	Errors
6.1-6.8	Ports 6.1-6.8	00-Oct-01 21:39:36	0%	28,544	0	64	0	0	0%	28,736	0	67	0	0
6.9-6.16	Ports 6.9-6.16	00-Oct-01 21:39:36	0%	28,544	0	64	0	0	0%	28,736	0	67	0	0
6.17-6.24	Ports 6.17-6.24	00-Oct-01 21:39:36	0%	28,544	0	64	0	0	0%	28,736	0	67	0	0
6.25-6.32	Ports 6.25-6.32	00-Oct-01 21:39:36	0%	28,544	0	64	0	0	0%	28,736	0	67	0	0
6.33-6.40	Ports 6.33-6.40	00-Oct-01 21:39:36	0%	28,544	0	64	0	0	0%	28,736	0	67	0	0
6.41-6.48	Ports 6.41-6.48	00-Oct-01 21:39:36	0%	28,544	0	64	0	0	0%	28,736	0	67	0	0

Clear Counters

4. Click Clear Counters to get a fresh view of the statistics being gathered. This resets all of the counters to zero so that you can track the counters from a particular point forward.

5. Select a port from the Name column to view statistics for that specific port. The Ethernet Interface Statistics dialog box opens (Figure 19-3).

Figure 19-3. Ethernet Interface Statistics Dialog Box

Available History Links (mm:ss) :

0:30 sample
30:0 sample

Ethernet Interface Statistics

Statistic	Total	Receive	Transmit
Utilization	0%	0%	0%
Bytes	57,280	28,544	28,736
Unicast Packets	0	0	0
Multicast Packets	131	64	67
Discards	0	0	0
Errors	0	0	0
Pause Frames	0	0	0

Error Detail

6. Select either 0:30 sample (30 second sample) or 30:0 sample (30 minute sample) from the Available History Links field. The Ethernet Interface Statistics dialog box opens with the sample you selected.

7. Refer to *Table 19-1* for an explanation of the Ethernet Interface Statistics Dialog Box fields:

Table 19-1. Ethernet Interface Statistics Dialog Box Fields

Statistic	Indicates	Actions
Sample	The sample number.	N/A
Interval Start	The date and time this log entry was made.	N/A
Utilization	Percentage of utilization.	The percentage of available bandwidth used by traffic.
Bytes	Raw number of octets received at the interface. Provides some indication of the amount of network bandwidth being used.	A sharp increase could indicate a need to reconfigure the network.
Packets	Counts the raw number of readable Ethernet packets of legal length received at the interface.	A sharp increase could indicate a need to reconfigure the network. (However, octets are a better indication of bandwidth utilization.)
Broadcasts	Broadcast packets are a normal part of network operation. For example, IP networks use broadcasts as part of Address Resolution Protocol (ARP) to resolve network addresses.	Uses monitoring to recognize oncoming broadcast storms. Broadcast storms occur when stations are creating traffic that generates more traffic. **Possible cause:** Broadcasts cause every host on a network segment to process the packet. Possible actions: • To prevent broadcast storms, use VLANs to limit the area of the network that each broadcast packet affects. In general, each VLAN creates a separate broadcast domain. More VLANs mean less proliferation of broadcast packets. • Monitor the broadcast rate of your network during normal operation. • Establish a baseline. • Use Rate Limiting to reduce broadcasts.

***Table 19-1. Ethernet Interface Statistics Dialog Box Fields** continued*

Statistic	Indicates	Actions
Multicasts	Normal during network operation. For example, multicast packets are to send target video streams to selected stations on the network, and are part of the operation of the Spanning Tree Protocol.	**Possible causes:** • Too many multicast frames can consume valuable network bandwidth. **Possible actions:** • Using Intelligent Multicasting can significantly reduce multicast traffic on individual ports. • Segmenting the network into smaller VLANs and routing between them can also help control proliferation of multicasts.
CRC (Cyclic Redundancy Check) or Alignment Errors	Counts of the number of times that the number of bits in a frame cannot be divided by 8 (that is, cannot be broken into legal octets), and that contain a Frame Check Sequence validation error. Typically caused by turning equipment on or off, and by noise on twisted pair segments. These errors can also result from configuring a network that does not comply with 802.3 standards. In a standards-compliant Ethernet network, CRC or alignment errors represent transit and receive bit errors. The Ethernet standard allows 1 in 10^8 bit error rate, but you should expect performance to be less than 1 in 10^{12} packets. Rates in excess of one error per one thousand packets indicate a serious problem.	**Possible causes**: • Defect at the transmitting station. • Turning equipment on or off. This should cause only a few errors. • Damaged cables. • Interference on network cabling. **Possible action**s (respectively): • Use port error statistics to isolate the problem. Check the transceiver or adapter card connected to the port where the problem seems to originate. Also check the cable and cable connections for damage. • Normal operation, no action required. • Check cables for damage. • Inspect cable runs to see if they are too close to noisy devices, and check for problems with network devices.

***Table 19-1. Ethernet Interface Statistics Dialog Box Fields** continued*

Statistic	Indicates	Actions
Undersized Packets	Count of packets with a valid CRC that violate the minimum Ethernet packet size. These malformed packets are most often the result of software errors.	**Possible cause:** Device or application creating non-compliant packets. **Possible action:** Use a network analyzer to identify the transceiver which at the source of the problem. If necessary, replace transceiver, network adapter, or station.
Oversized Packets	Count of packets with a valid CRC that violate the maximum Ethernet packet size. These malformed packets are most often the result of software errors.	**Possible cause:** Device or application creating non-compliant packets. **Possible action:** Use a network analyzer to identify the transceiver which at the source of the problem. If necessary, replace transceiver, network adapter, or station.
Fragments	Fragments or runts result from normal collision activity in Ethernet networks. A runt packet is an incomplete packet that is long enough to be detected by an Ethernet interface.	**Possible causes**: • Interference on network cabling. • A Transceiver attached to the Repeater is generating Signal Quality Errors (SQE). **Possible actions (respectively)**: • Inspect cable runs to see if they are too close to noisy devices, and check for problems with network devices. • Disable SQE on the Transceiver.

***Table 19-1. Ethernet Interface Statistics Dialog Box Fields** continued*

Statistic	Indicates	Actions
Jabbers	Jabbers indicate that devices on the networks are sending improper electrical signals. Because Ethernet uses electrical signalling to determine whether or not it is okay to transmit, a jabber condition can halt all traffic on a segment.	**Possible causes**: • Bad network interface card • Repeater network with looped traffic **Possible actions (respectively):** • Replace the network interface card. • Rewire network to remove the loop.
Collisions (half-duplex links only)	Counts number of times that packets have collided on the network. Collisions increase as network use of shared segments increases. Therefore, if the collision rate increases without an increase of network use, it might indicate a problem. Guidelines for appropriate collision rates are: • 10 percent: Normal collision rate for shared Ethernet segment. • 30 percent: Collisions begin to interfere with performance. • 70 percent: Practical limit for network to remain functioning. A full-duplex link should not show collision activity. Collisions are rare in a switched network, unless your switched segments attach to multiple ends stations (a legal configuration option).	**Possible causes**: • Busy network • Broken adapter (not listening before broadcasting) • Network loop **Possible actions (respectively)**: • If you have multiple stations on a switch segment, reconfigure network into segments with fewer stations. • Isolate each adapter to see if the problem ceases. • Activate spanning tree to resolve loops automatically. • Ensure that there are no connections to the same station where both connections are simultaneously active.

Viewing Network Statistics Using the CLI

To view network statistics using the CLI, enter the following command in Priv mode:

```
cajun# show ethernet counters <cr|mod-num|mod-
swport-spec>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

Setting Up a Mirror Port

Configuring an RMON mirror port allows you to mirror traffic from a port or set of ports to a specific mirror port, where you can attach a sniffer or RMON probe. The switch supports a single mirror port and a single source port for each switch fabric port. For example, 20-port Fast Ethernet cards have two fabric ports (one for ports 1 through 10, one for ports 11 through 20). You can set up a single source port and a single mirror port for each set of ports associated with a fabric port. You can also choose to mirror all traffic from a particular fabric port to the mirror port, or set up multiple source ports to mirror traffic to a single mirror port.

Packets addressed to the CPU, such as pings, are duplicated out of the mirror port. Tagged packets that are sent into a source port with a VLAN ID to which the source port is not bound, are not transmitted out the mirror port. VLAN tag information is not propagated to the mirror port.

*** Note:** To prevent unnecessary traffic flooding on a mirror port, put the mirror port on the same VLAN as the source port.

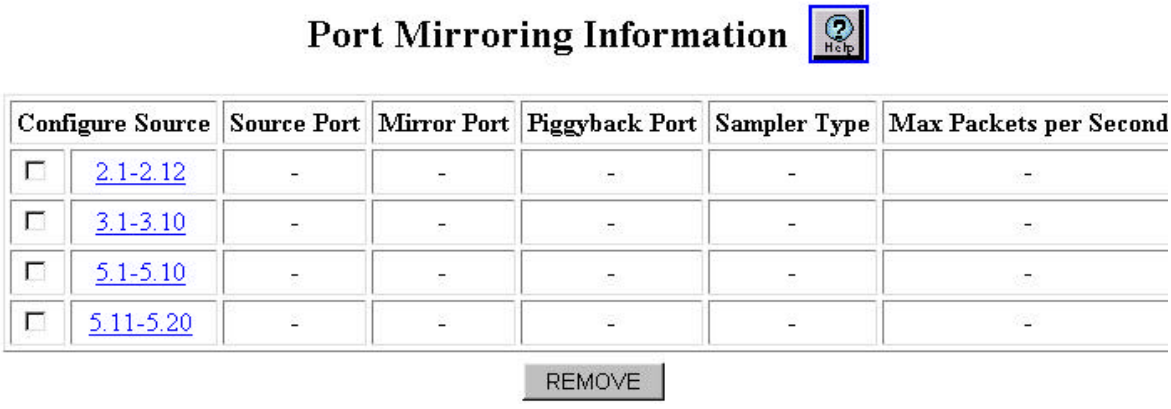
You can setup a mirror port using either the web agent or the CLI.

Setting Up a Mirror Port Using the Web Agent

To set up an RMON mirror port using the web agent:

1. Select Sampling from the Port Mirroring group on the web agent window. The Port Mirroring Information dialog box opens (Figure 19-4).

Figure 19-4. Port Mirroring Information Dialog Box



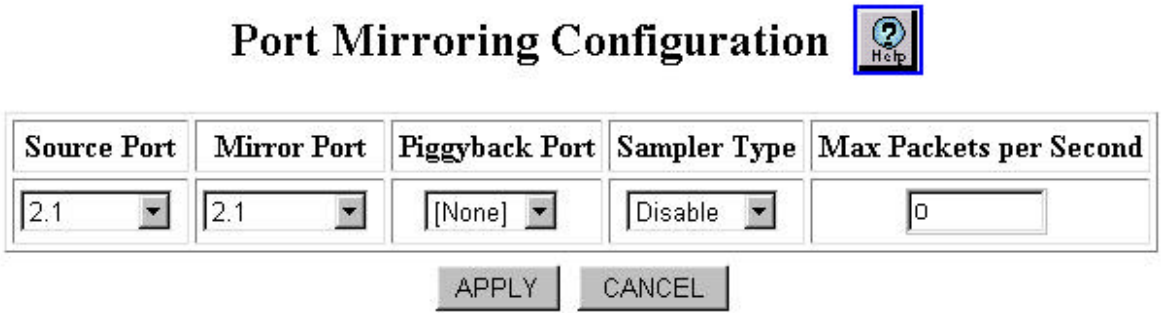
2. Refer to Table 19-2 for an explanation of the Port Mirroring Information dialog box parameters.

Table 19-2. Port Mirroring Information Dialog Box Parameters

Parameter	Definition
Configure Source	Select the configuration source port. Provides a link to the Port Mirroring Configuration dialog box.
Source Port	Displays the port under investigation.
Mirror Port	Displays the port that transmits mirrored data.
Mirror Port Name	Displays the name of the mirror port device.
Piggyback Port	Displays the name of the port that is used for bi-directional port mirroring. When used as a mirror port, it is unavailable for other uses.
Sampler Type	Displays the speed of sampling that is performed for source port traffic.
Max Packets per Second	Displays the maximum number of packets per second that are served by the mirror port.

3. Select a source port for traffic from the Configure Source column. The Port Mirroring Configuration dialog box opens (Figure 19-5).

Figure 19-5. Port Mirroring Configuration Dialog Box



4. Refer to Table 19-3for an explanation of the Port Mirroring Configuration dialog box parameters:

Table 19-3. Port Mirroring Configuration Dialog Box Parameters

Parameter	Definition
Source Port(s)	List of available selections. You can select a particular source port associated with the selected fabric port. You can also select all ports. **Note:** To mirror inbound traffic only, select a source port and a mirror port, not a piggyback port.
Mirror Port	Displays the port from which you want to send the traffic. This port can be on another module in the switch. Once a specific port associated with a fabric port has been designated a mirror port, other ports associated with that fabric port no longer appear on the selection list.

Table 19-3. Port Mirroring Configuration Dialog Box Parameters *continued*

Parameter	Definition
Piggyback Port	Port used to enable bi-directional port mirroring. If no piggyback port is specified, only received traffic from the source port will go to the mirror port. The piggyback port should have the same bandwidth as the source port. Only one port per fabric can be used as a piggyback port. Sampling rates have no effect on transmitted information. **Considerations:** • You cannot use a port that has been designated as a piggyback port. • Once a port has been designated as a piggyback port, the link light is turned on, even if there is no connection on the selected port. • The piggyback port is displayed in place of the source port in the VLAN menu. • If the source and piggyback ports are at a higher bandwidth than the mirror port's bandwidth, the traffic on the source port may exceed the bandwidth that the mirror port can handle. • The piggyback port will always show that it is using multi-layer tagging. • A spanning tree topology change occurs when you change a piggyback port. • Piggyback ports display in certain views of the Cajun P550 Switch user interface where you typically expect to find information about a source port. For example, the VLAN Switch Ports list, which displays the list of ports associated with a VLAN, includes the piggyback port but not the source port. In the Intelligent Multicast Session Search and Static Multicast Sessions views, the piggyback port displays in place of the source port when piggyback port mirroring is enabled. Note: To mirror outbound traffic only, select a source, mirror, and piggyback port. Set the sampling to disable. Since disabling sampling only applies to inbound traffic, only outbound traffic is received.

Table 19-3. Port Mirroring Configuration Dialog Box Parameters *continued*

Parameter	Definition
Sampler Type*	Selects how often you want the mirror port to receive traffic samples: • **Always** - sends all samples. • **Periodic** - sends samples at the interval described below. • **Disabled** - shuts off traffic samples to the mirror port, but keeps the association intact.
Max Packets per Second	Displays the number of packets per second that are served by the mirror port.

* Sampling only applies to inbound traffic.

Setting Up a Mirror Port Using the CLI

To set up an RMON mirror port using the CLI, enter the following command from Configure mode:

```
cajun(configure)# set port mirror <mod-port-range>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

20 Tuning Your Switch Performance

Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations. Buffer management features help you to optimize traffic throughput through the switch fabric.

This chapter provides the following information:

- How Queues Work
- Managing Buffers and Queues

How Queues Work

Frames are buffered in the I/O modules, before and after traversing the switch. Each queue can hold 256K bytes. (Architecturally they can support up to 1 MB each).

Each buffer is divided into two queues, one for High-priority Traffic and one for Normal-priority Traffic. The factory default is for the high-priority queue uses 20% (51K) of the buffer. The normal-priority queue uses the remaining 80% (205K). These values can be modified using either the Web Agent or SNMP.

*** Note:** When you change these values, you must reboot the switch before they can take effect.

Less buffer memory gets assigned to the high-priority queue because the high-priority queue gets serviced more frequently than the normal-priority queue. Since a frame spends less time on the high-priority queue, less buffer space is required for the queue.

The Service Ratio can be chosen to match traffic patterns and performance requirements using a weighted round robin scheduling algorithm. The available service ratios of the algorithm are defined in "*Managing Buffers and Queues*". The factory default service ratio for fabric ports is 999/1. The factory default service ratio for physical ports is 1023 to 1. If there is traffic to be serviced from both the high- and normal-priority queues, 999 packets of high-priority traffic will be processed for each normal-priority packet.

When the high-priority queue fills up, incoming frames are dropped. The philosophy is if a high-priority frame is going to be late, it is not worth sending it at all. The normal-priority queue uses either IEEE 802.3X PAUSE (variable timed XOFF) flow control or Half Duplex collisions to shut off incoming frames before the queue overflows.

The switch implements two flow control disciplines along the entire path that frames travel. The default case is that when output buffers fill up, frames destined for a particular buffer will be dropped. This should only occur in a case where the output port is very congested. However, there is an optional mode which in which normal-priority frames are never dropped inside the switch. In this mode, input buffers may fill up. If they do, the affected input ports may use flow control to temporarily halt traffic from neighboring switches.

Managing Buffers and Queues

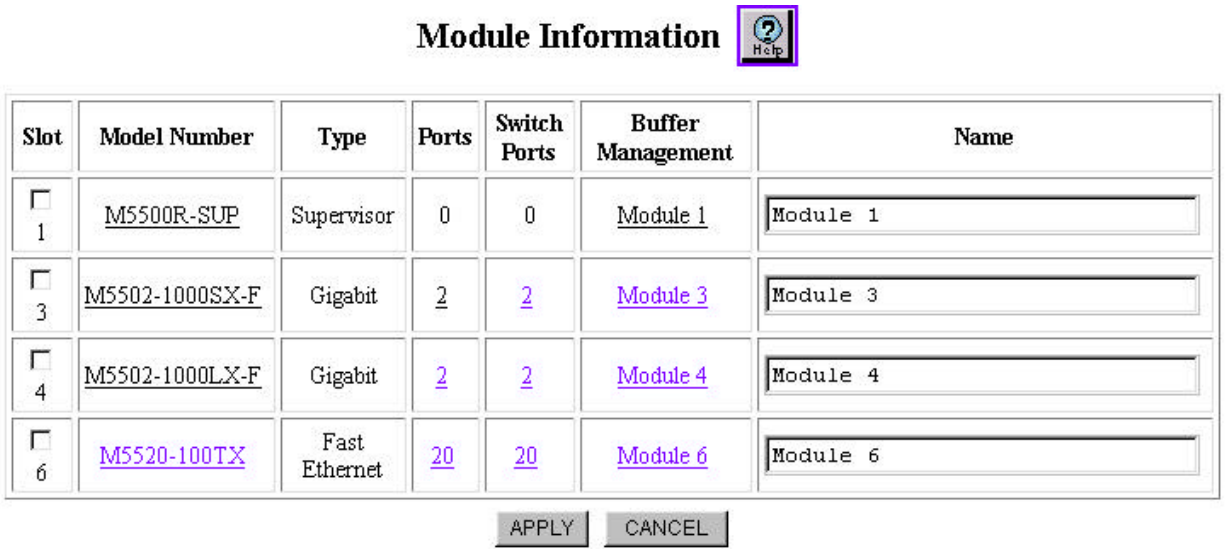
You can manage buffers and queues using either the web agent or the CLI.

Managing Buffers and Queues Using the Web Agent

To manage buffers and queues using the web agent:

1. Select Configuration from the Modules & Ports group on the web agent window. The Module Information dialog box opens (Figure 20-1).

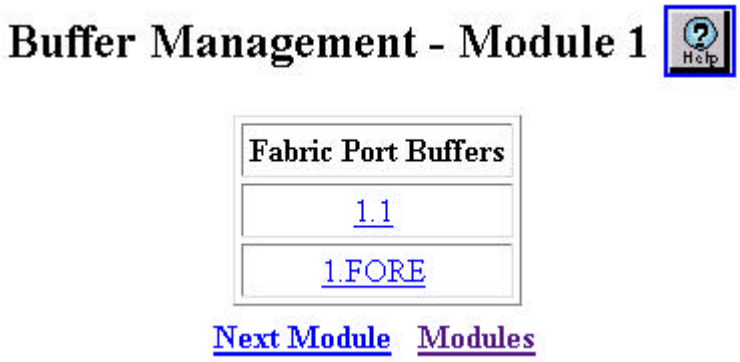
Figure 20-1. Module Information Dialog Box



2. Select the checkbox for the module whose buffers you want to manage from the Select column.

3. Select the Module number for that module from the Buffer Management column. The Buffer Management dialog box opens (Figure 20-2).

Figure 20-2. Buffer Management Dialog Box



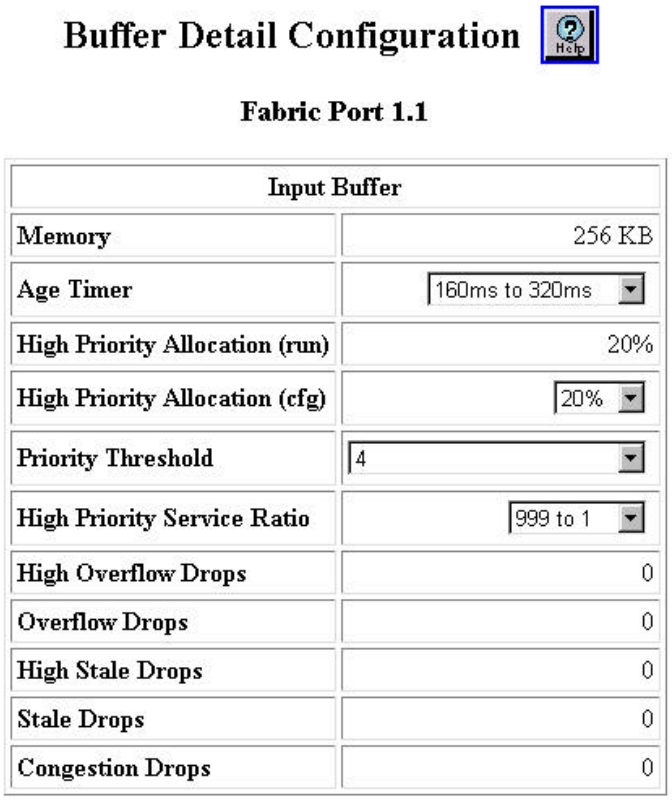
4. Refer to Table 20-1 for an explanation of the Buffer Management dialog box parameters.

Table 20-1. Buffer Management Dialog Box Parameters

Parameter	Definition
Fabric Port Buffers	Displays the port's fabric port buffers and allows you to open the **Buffer Detail Configuration** dialog box for the selected module. Service ratios: • 3 to 1 • 99 to 1 • 999 to 1 • 9999 to 1
Physical Port Buffers	Displays the port's physical port buffers if available. The buffer ratios are: • 31 to 1 • 63 to 1 • 127 to 1 • 255 to 1 • 511 to 1 • 1023 to 1 • 2047 to 1 • 4095 to 1 • 8191 to 1 • 16383 to 1 • 32767 to 1

5. Select the Fabric Port Buffer number whose associated buffers you want to manage. The Buffer Detail Configuration dialog box for that fabric port opens (Figure 20-3).

Figure 20-3. Buffer Detail Configuration Dialog Box



6. Refer to Table 20-2 for an explanation of the Buffer Detail Configuration dialog box input and output fields:

Table 20-2. Buffer Detail Configuration Dialog Box Parameters

Parameter	Definition ...
Memory	Displays the amount of physical memory associated with this buffer.
Age Timer	Displays the amount of time a packet remains in the queue before being discarded as a stale packet. You may want to increase the timer value for ports connected to 10 MB/s ports, particularly 10 MB/s shared media, because you may want to queue packets longer before discarding them.

Table 20-2. Buffer Detail Configuration Dialog Box Parameters
continued

Parameter	Definition ...
High Priority Allocation	Displays the percent of the buffer's queuing space allotted to high priority traffic. Because the high-priority queue is serviced more frequently than the normal priority queue, raising this value may not necessarily provide better service. In fact, if you are using the high-priority queue for delay-sensitive traffic, you may want to reduce the amount of memory devoted to the high-priority queue. This ensures that packets that cannot be delivered in a timely manner are discarded. If you want the high priority queue to guarantee delivery of as many packets as possible, regardless of delay, increase this value. The change does not take effect until you reset the switch.
Priority Threshold	Allows you to set this parameter to the value at which the Cajun P550 switch starts sending packets to the high-priority queue. The default value (4) causes all traffic with a priority greater than or equal to 4 (4, 5, 6, and 7) to be assigned to the high-priority queue. Priority schemes have more than two queues (the IEEE allows up to 8, numbered 0 through 7). Avaya recommends that you do not change this parameter.
High Priority Service Ratio	Allows you to set how many times the high priority queue is serviced for each time the low priority queue is serviced. The ideal value changes from queue to queue, but the goal is to ensure that traffic mix guarantees optimal mix between high-priority and best effort traffic.
High and Normal Overflow Drops	Displays the number of packets dropped because the associated buffer is full. Indicates that the device immediately before the queue is processing traffic faster than the next downstream element can process the same volume of traffic. For example, overflow drops on the input buffer indicate that traffic is arriving faster than the switch matrix can process it. Overflow drops on the output buffers indicates that the output port cannot handle the volume of the load being offered.
High and Normal Stale Drops	Displays the number of packets dropped because they timed out waiting for service (using the age timer value). In the high-priority queue, this can help determine how efficiently the switch is processing "better never than late" traffic. Excessive stale drops on the high-priority queue may indicate the need to increase the service ratio on the high-priority queue.
Congestion Drops	Displays the number of packets dropped because the switch controller has sensed congestion at the outbound port.

7. Repeat Steps 1-4 to tune Physical Port (Fast Ethernet) buffers. Physical Port ports have additional buffers on both the input and output ports.

8. Click APPLY to save your changes, or CANCEL to restore previous settings.

Managing Buffers and Queues Using the CLI

To manage buffers and queues using the CLI, enter the following command from **Configure** mode:

```
cajun(configure)# set buffering port <mod-swport-spec>
```

Refer to the *Cajun™ P550™/P880/P882 Command Line Interface Reference Guide for Version 5.0* for details about this command.

A Downloading New Operational Code to the Switch

Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- Upgrading from a Previous Version
- Downloading a Software Image
- Selecting the Image for Reboot
- Resetting the Switch

Upgrading from a Previous Version

The P550/P880/P882 switches all handle configuration files differently from previous releases. In previous releases, all configuration information is contained in a `startup.txt` file that is stored in NVRAM on the switch. Previous versions used `*.cfg` files that contained information about multiple types of configuration data.

When you upgrade the switch's embedded software to version 5.0, the previous software version is remains in the APP1 memory location, and the version 5.0 software image is installed into APP2. If you want to save the previous version on the switch for a potential downgrade, find out which APP you booted from, then load the new image into the other APP. For example, if you boot a previous version from APP1, download version 5.0 into APP2.

Saving the Previous Configuration

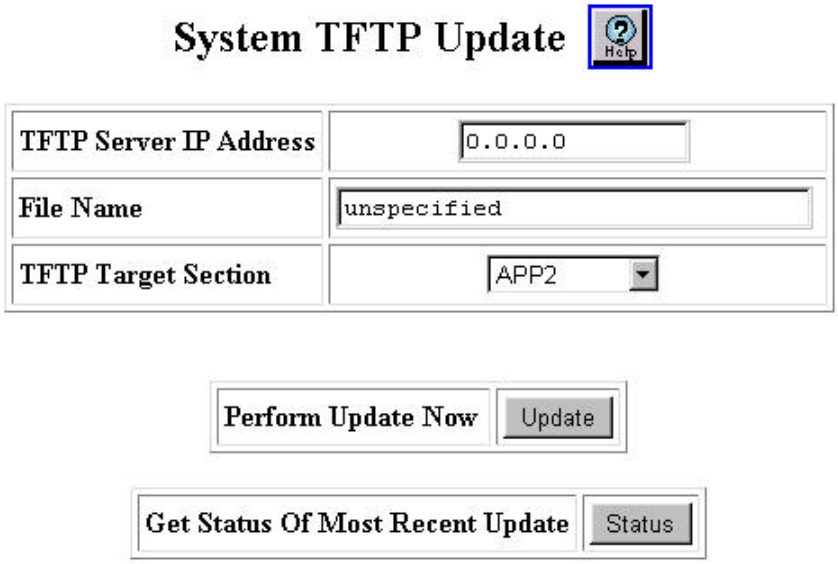
Before you upgrade your system, save your previous configuration to a file or directory on a TFTP server. You can do this using either the web agent or the CLI.

Saving the Previous Configuration Using the Web Agent

To save your current configuration using the Web Agent:

1. Select **System** from the **System > Memory >TFTP Update** group on the web agent window. The **System TFTP Update** dialog box opens (Figure A-1).

Figure A-1. System TFTP Update Dialog Box



2. Enter the **IP address** of the TFTP server to which you will save the previous configuration in the **TFTP Server IP Address** field.

3. Enter a file name for the previous configuration file in the **File Name** field.

4. Select **Save Configuration** from the **TFTP Target Section** pull-down menu.

5. Click **Update** in the **Perform Update Now** field.

6. Click **Status** in **Get Status of Most Recent Update** field to verify that the configuration file was saved properly.

Saving the Previous Configuration Using the CLI

To save your current configuration using the CLI, enter the following command in **Priv** mode:

```
># copy tftp <filename-opt-path>
```

Refer to the Cajun™ P550™/P880 Command Line Interface Reference Guide for Version 5.0 for details about this command.

Downloading a Software Image

You can download the version 5.0 software image from a TFTP server to an APP location using either the web agent or the CLI.

Downloading a Software Image Using the Web Agent

To download the version 5.0 software image from a TFTP server to an APP location using the web agent:

1. Select **System** from the **System > Memory >TFTP Update** group on the web agent window. The **System TFTP Update** dialog box opens (Figure A-1).
2. Enter the IP address of the TFTP server that has the version 5.0 software image in the **TFTP Server IP Address** field.
3. Enter one of the following in the **File Name** field:
   - **m5500_v5.0.0.bin** to download version 5.0 for the Cajun P550 switch (layer 2)
   - **m5500r_v5.0.0.bin** to download version 5.0 for the Cajun P550R switch (layer 3)
   - **m8800_v5.0.0.bin** to download version 5.0 for the Cajun P880 switch
4. Select the location where you want to download the version 5.0 software image from the **TFTP Target Section** field pull-down menu.
5. Click **Update** in **Perform Update Now** field.
6. Click **Status** in **Get Status of Most Recent Update** field to verify that the new image downloaded properly.

Downloading a Software Image Using the CLI

To download the version 5.0 software image from a TFTP server to an APP location using the CLI, enter the following command in **legacy-cli** mode:

```
> fep get

   This command reads and displays information
   about the software image currently stored
   in APP1 and APP2.


> download <APPname> <IP address> <file name>
```

Refer to the Cajun™ P550™/P880 Command Line Interface Reference Guide for Version 5.0 for details about these commands.

Selecting the Image for Reboot

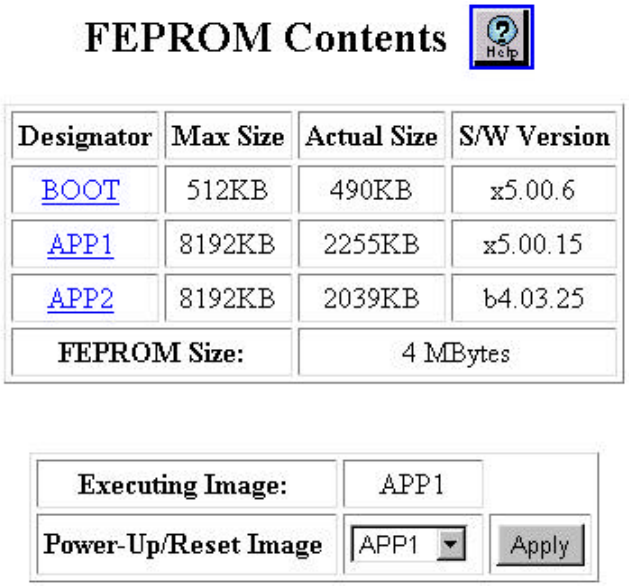
You can view and power-up the downloaded software image using either the web agent or the CLI.

Selecting the Image for Reboot Using the Web Agent

To view and power up the downloaded image using the web agent:

1. Select **FEPROM** from the **System > Memory** group on the web agent window. The **FEPROM** dialog box opens (Figure A-2).

Figure A-2. FEPROM Contents Dialog Box



2. Select the APP location into which you downloaded the version 5.0 software image in the **Power Up/Reset Image** field pull-down menu.

3. Click **APPLY** from the **Power Up/Reset Image** field.

Selecting the Image for Reboot Using the CLI

To set the location from which you download the software using the CLI, enter the following command from the legacy-cli:

```
>fep set <APPname>
```

Refer to the Cajun™ P550™/P880 Command Line Interface Reference Guide for Version 5.0 for details about these commands.

Resetting the Switch

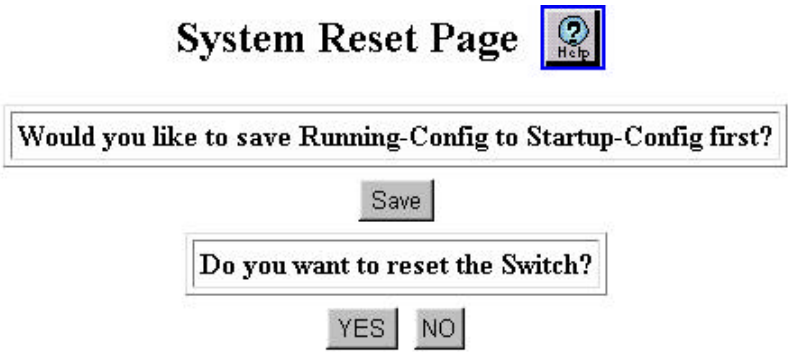
You can reset the Cajun P550/P880 switch using either the web agent or the CLI.

Resetting the Switch Using the Web Agent

To reset the switch using the web agent after downloading the version 5.0 software image:

1. Select **System Reset** from the **System** group on the web agent window. The **System Reset Page** dialog box opens (Figure A-3).

Figure A-3. System Reset Page Dialog Box



2. Click **Yes** in response to the question, **Do you want to reset the switch?**. The switch resets with the selected version.

Resetting the Switch Using the CLI

To reset the switch using the CLI after downloading the version 5.0 software image, enter the following command in Legacy-cli mode:

```
> reset
```

Refer to the Cajun™ P550™/P880 Command Line Interface Reference Guide for Version 5.0 for details about these commands.

B Boot Mode

Boot Mode is a special mode for the Cajun P550/P880 switches. Boot mode is used to:

- recover your password
- download new operational code

Accessing BOOT Mode

You can access BOOT mode during Power Up or when both Operational Images in APP1 and App2 are corrupted.

Accessing BOOT Mode During Power Up

To access BOOT mode during power up:

1. Power-Off the Switch.
2. Connect a console to the supervisor Module (refer to the *Cajun P550/P880 Switch Installation Guide*, "Chapter 3, Configuration").
3. Press and Hold the DISPLAY button on the supervisor module
4. Power-on the switch

Accessing BOOT Mode with Corrupted Operational Images

The Cajun P550/P880 switch will automatically come up in BOOT mode if both operational images are corrupted.

You will see the following output on your console:

```
Starting the boot system, please wait.
Initializing the event subsystem ... done
Initializing the platform ... done


Starting up threads ...
    Periodic Task
    Network Interface
    Front Panel Display
    Download
    Command Line Parser

Boot process complete - system is now operational.

Boot Software Revision: V5.0

Press Ctrl-P for previous command, Ctrl-N for next
command


download   Download to FEPROM
feprom     Flash EPROM configuration
initLogins Restore default passwords
ip         IP Configuration
manuf      Get/Set MAC address
nvram      Initializes NV RAM-diags run upon reboot
peek       Read from memory
ping       Ping host [tries] [delay]
poke       Write to memory
reset      Reset System

Boot>
```

Password Recovery

The following command is used to reset the switch to the factory default passwords.

initLogins

Syntax

```
Boot> initLogins set <0=no change, 1=factory
default>
```

Description

Using a value of zero will retain the current passwords in NVRAM upon resetting the switch. Using a value of one will restore the factory default passwords in NVRAM upon resetting the switch.

Downloading New Operational Code

To download new operational code in BOOT mode into APP1 or APP2.

*** Note:** The P550/P880 does not have an IP address assigned to the console ethernet port when it comes up in BOOT mode. Therefore, a user must assign an IP address (and default gateway) to the ethernet console port prior to attempting the TFTP download of a new operational image.

1. Ensure the ethernet console port is connected to the network for a TFTP transfer (refer to the *Cajun P550/P880 Switch Installation Guide*, "Chapter 3, Configuration").

2. Enter the following command to assign an IP address to the ethernet console port:

   ```
   Boot> ip address <ip address> <ip mask>
   ```

3. Enter the following command to assign a default gateway to the ethernet console port (if necessary):

   ```
   Boot> ip default_gateway <ip address>
   ```

4. Enter the following command to download new operational code to APP1 or APP2:

   ```
   Boot> download <app1|app2> <serverIP>
   <filename>
   ```

5. Enter the following command to set the switch to boot from the appropriate image stored in APP1 or APP2

```
Boot> feprom set <app1|app2>
```

6. Enter the following command to reset the switch:

```
Boot> reset
```

C Supported MIB Groups

Management Information Bases (MIBs) Supported by Layer 2 and Multilayer Switches

The following section lists, by protocol, public and private MIBs supported by the P550/P7880/P882 switches. Note that all MIBs supported by Layer 2 switches also are supported by the multilayer switch. For information about additional MIBs supported by the P550R, refer to “MIBs Supported by the Multilayer Switch” on page 2.

IPX Interface MIBs

The following public and private MIBs define the attributes of IPX interfaces.

The Novel MIB is not currently supported

Private IPX Interface MIBs

The following private IPX interface MIBs are supported:

- cjnipxifmgmt.mib
- cjnipx.mib
- cjnipxrip.mib
- cjnipxsap.mib

Prominet MIB

The following components of the private Prominet MIB are supported:

- ProminetMIB.txt
- cjnSwitchRoot.mib
- cjnRoot.mib

IEEE 802.3 MAU Management

RFC 1155.smi is supported.

IEEE 802.3 Statistics Group

RFC 1398.mib is supported.

Bridge MIB

RFC 1493.mib is supported.

SNMPv2

RFC 1907.mib is supported.

RMON

RFC 1757.mib is supported.

MIBs Supported by the Multilayer Switch

The following section lists, by protocol, public and private Management Information Bases (MIBs) supported by the Cajun P550R switch, the multilayer 3 switch. For information about additional MIBs supported by the P550R switch, refer to “Management Information Bases (MIBs) Supported by Layer 2 and Multilayer Switches” on page 1.

RIP Version 1.0 and 2.0

Standard MIB

RFC 1724 is supported.

Private MIB

The private MIB, cjniprip.mib is supported.

OSPF Version 2.0

Standard MIB

RFC 1850 is supported.

Private MIB

The private MIB cjnospf.mib is supported.

VRRP

Standard MIB

The current draft of the Virtual Redundancy Router Protocol (VRRP) MIB is supported: draft-ietf-vrrp-mib-04.mib.

Private MIB

The private cjniplrrp.mib is supported.

IGMP

Standard MIB

The current draft of the Internet Group Membership Protocol (IGMP) MIB is supported: draft-ietf-idmr-igmp-mib-07.mib.

Private MIB

The private cjnigmp.mib is supported.

IP Interface

The private cjhnipifmgmt.mib is supported.

IP Version 4.0 and Services

Standard MIB

The following standard MIBs for Internet Protocol version 4.0 and services are supported:

- RFC 1213.mib
- RFC 2011.mib
- RFC 2012.mib
- RFC 2013.mib

Private MIB

The following private MIBs are supported for Internet Protocol version 4.0 and services:

- cjnipv4.mib
- cjnipv4serv.mib

IP Forwarding/Route Table

Standard MIB RFC 2096.mib is supported.

Private MIB The private cjnipfwd.mib is supported.

DVMRP

Standard MIB The current draft of the DVMRP MIB is supported: draft-thaler-dvmrp-mib-9.mib.

Private MIB The private cjndvmrp.mib is supported.

AppleTalk

Standard MIB RFC 1243.mib is supported.

Private MIB The private cjnatalk.mib is supported.

IP Access List

The private MIB that defines IP access list format, cjnipalist.mib, is supported.

Policy Capability MIB for LDAP

The private MIB that defines policy capabilities for the Lightweight Directory Access Protocol (LDAP), cjnpolicycap.mib, is supported.

Load MIB Overview

The Load MIB defines upload, download and copy of application software and configuration information.

The genOperations group

Each row in the genOpTable represents an operation that this system can perform. A walk of this table should provide a list of available operation that can be performed by the system. The genOpTable contains all configuration information necessary to perform upload, download, and copy operations within the system. Source, Destination, operational trigger, operational status and error logging information is contained on a per row basis (each row again representing an operation that this table can perform).

The genApplication Group

Table of Application (FILE) entries. Each row uniquely defines an application in the system. Applications can be defined as any entity that can be read or written from or to the system. This includes software images, boot code, configuration files, prom code. Each row contains information used to catalog the application (FILE) entries present in the system. A walk of the genAppFileTable should provide a directory-like listing of all application software, boot code, configuration files and misc. accessible by the embedded software in the system. Each entry contains information about the application such as type, size, version number and date stamp.

MIB Specifications

```
-- MIB: Avaya Common Download / Upload MIB

-- Version: 1.3.4                04, October 2000

-- Copyright 2000 Avaya Inc., Ltd.

-- All Rights Reserved.

-- Reproduction of this document is authorized on condition

-- that the foregoing copyright notice is included.

-- This Avaya Inc. SNMP Management Information Base

-- Specification embodies Avaya Technologies confidential and

-- Proprietary intellectual property.  Avaya Inc. retains all

-- Title and ownership in the Specification, including any revisions

-- It is Avaya's intent to encourage the widespread use of this
-- Specification in connection with the management of Avaya Inc.
-- products.
```

-- Avaya Inc. grants vendors, end-users, and other interested parties

-- a non-exclusive license to use this Specification in connection

-- with the management of Avaya Technologies products.

-- This Specification is supplied "as is," and Avaya Inc. makes

-- no warranty, either express or implied, as to the use,

-- operation, condition, or performance of the Specification.

-- **Overview:**

-- The Load MIB defines upload, download and copy of application software

-- and configuration information.

-- T**he genOperations group**

-- Each row in the genOpTable represents an operation that this system can

-- perform. A walk of this table should provide an list of available operation

-- that can be performed by the system. The genOpTable contains all configuration

-- information nessary to perform upload, download, and copy operations within the

-- system. Source, Destination, operational trigger, opertional status and error

-- logging information is contained on a per row basis (each row again representing

-- an operation that this table can perform.

-- **The genApplication Group**

-- Table of Application (FILE) entries. Each row uniquely defines an application

```
-- in the system.  Applications can be defined as any entity that can
be read or

-- written from or to the system.  This includes software images,
boot code,

-- configuration files, prom code, etc. Each row contains
information used to

-- catalog the application(FILE) entries present in the system. A
walk of the

-- genAppFileTable should provide a directory-like listing of all
application

-- software, bootcode, configuration files and misc. accessable
embedded software

-- in the system.  Each entry contains information about the
application such as

-- type, size, version number and date stamp.

LOAD-MIB DEFINITIONS ::= BEGIN

IMPORTS

        MODULE-IDENTITY, OBJECT-TYPE,

        enterprises, IpAddress, Integer32        FROM SNMPv2-SMI

        DisplayString, RowStatus                 FROM SNMPv2-TC;


Avaya       OBJECT IDENTIFIER ::= { enterprises 1751 }

products    OBJECT IDENTIFIER ::= { Avaya 1 }

mibs        OBJECT IDENTIFIER ::= { Avaya 2 }


load   MODULE-IDENTITY

     LAST-UPDATED "9904230000Z" -- 23 Apr. 1999"
```

```
        ORGANIZATION "Avaya Inc."
        CONTACT-INFO
              "Itai Zilbershtein -- izilbers@Avaya.com
               Yigal Nehaysi -- ynehaysi@Avaya.com
               Erick Crowell -- ecrowell@Avaya.com
               Ira Steckler -- isteckler@Avaya.com"

        DESCRIPTION
              "Avaya Common Download / Upload Private MIB"
        ::= { mibs 53 }

-- Groups in the Load mib

        genOperations   OBJECT IDENTIFIER ::= { load 1 }
        genApplications OBJECT IDENTIFIER ::= { load 2 }

-- The genOperations group
--
genLoadNumberOfSession OBJECT-TYPE
        SYNTAX  Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
```

"The number of operational sessions in progress in this system"

::= { genOperations 1 }

genOpTable OBJECT-TYPE

SYNTAX SEQUENCE OF GenOpEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Table of configuration attributes which define the operational

functions and the results on a per module basis. This group provides

the mechanism by which available operations are initiated, monitored

and reported."

::= { genOperations 2 }

genOpEntry OBJECT-TYPE

SYNTAX GenOpEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An entry in the table, containing data about a single modules operations."

INDEX { genOpModuleId , genOpIndex }

::= { genOpTable 1 }

```
GenOpEntry ::=
    SEQUENCE {
        genOpModuleId               INTEGER,
        genOpIndex                  INTEGER,
        genOpRunningState           INTEGER,
        genOpSourceIndex            Integer32,
        genOpDestIndex              Integer32,
        genOpServerIP               IpAddress,
        genOpUserName               DisplayString,
        genOpPassword               OCTET STRING,
        genOpProtocolType           INTEGER,
        genOpFileName               DisplayString,
        genOpRunningStateDisplay DisplayString,
        genOpLastFailureIndex    INTEGER,
        genOpLastFailureDisplay  DisplayString,
        genOpLastWarningDisplay  DisplayString,
        genOpErrorLogIndex          Integer32,
        genOpResetSupported         INTEGER,
        genOpEnableReset            INTEGER,
        genOpNextBootImageIndex  Integer32,
        genOpLastBootImageIndex  Integer32,
        genOpFileSystemType      INTEGER,
    genOpReportSpecificFlags INTEGER,
```

```
        genOpOctetsReceived      INTEGER

                }


genOpModuleId OBJECT-TYPE

        SYNTAX INTEGER (1..255)

        MAX-ACCESS read-only

        STATUS current

        DESCRIPTION

       "Index which identifies the module inside the chassis for which
this

        entry contains information. Equals the number of the slot by
which

        the group is accessed or the stackable index."

        ::= { genOpEntry 1 }


genOpIndex OBJECT-TYPE

        SYNTAX INTEGER {

                uploadConfig(1),

                downloadConfig(2),

                report(3),

                uploadSoftware(4),

                downloadSoftware(5),

                localConfigFileCopy(6),

                localSWFileCopy(7),
```

uploadLogfile(8),

eraseFile(9),

show(10)

}

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Index to identify the operation supported by this row entry. Each operation

type that is supported by this module should be represented by a unique row

in this MIB Table. A walk of this MIB table should reveal all the operations

that are supported by the device.

The operations supported are:

uploadConfig --

The 'genOpDestIndex' should be set to 0 (to indicate destination of server),

the 'genOpServerIP' should be set to the server to which the config will be

saved.

the 'genOpProtocolType' should be set to the IP protocol used to transport

the file.

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the configFile

you are uploading.

downloadConfig --

The 'genOpDestIndex' should be set to the 'genAppFileId' of the configFile

you are download to (if one does not exist you'll need to RowCreate it

in the 'genAppFileTable'),

the 'genOpServerIP' should be set to the server from which the config will

be copied,

the 'genOpProtocolType' should be set to the IP protocol used to transport

the file,

the 'genOpSourceIndex' should be set to 0 (to indicate source of server),

report --

uploadSoftware --

The 'genOpDestIndex' should be set to 0 (to indicate destination of server),

the 'genOpServerIP' should be set to the server to which the config will be

saved,

the 'genOpProtocolType' should be set to the IP protocol used to transport

the file,

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the software

File you are uploading.

downloadSoftware --

The 'genOpDestIndex' should be set to the 'genAppFileId' of the software File

you are download to (if one does not exist you'll need to RowCreate it in the

'genAppFileTable'),

the 'genOpServerIP' should be set to the server from which the config will be copied,

the 'genOpProtocolType' should be set to the IP protocol used to transport the file,

the 'genOpSourceIndex' should be set to 0 (to indicate source of server).

localConfigFileCopy -- (using a 'genOpType' of 'localPeerTransport')

The 'genOpDestIndex' should be set to the 'genAppFileId' of the config File

you are copying to (if one does not exist you'll need to RowCreate it in the

'genAppFileTable'),

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the config File

you are copying from.

the 'genOpServerIP' should be set to NULL,

the 'genOpProtocolType' should be set to 'localPeerTransport',

localSWFileCopy -- (using a 'genOpType' of 'localPeerTransport')

The 'genOpDestIndex' should be set to the 'genAppFileId' of the software File

you are copying to (if one does not exist you'll need to RowCreate it in the

'genAppFileTable'),

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the software File

you are copying from.

the 'genOpServerIP' should be set to NULL,

the 'genOpProtocolType' should be set to 'localPeerTransport',

localConfigFileCopy -- (using a 'genOpType' of 'localServerTransport')

The 'genOpDestIndex' should be set to the 'genAppFileId' of the config File

you are copying to (if one does not exist you'll need to RowCreate it in the

'genAppFileTable') or ZERO (0) if copying to a localServer,

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the config File

you are copying from or ZERO (0) if copying from a localServer.

the 'genOpServerIP' should be set to the address of the local server,

the 'genOpProtocolType' should be set to 'localServerTransport',

localSWFileCopy -- (using a 'genOpType' of 'localServerTransport')

The 'genOpDestIndex' should be set to the 'genAppFileId' of the software File

you are copying to (if one does not exist you'll need to RowCreate it in the

'genAppFileTable'),

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the software File

you are copying from.

the 'genOpServerIP' should be set to the address of the local server,

the 'genOpProtocolType' should be set to 'localServerTransport',

uploadLogfile --

The 'genOpDestIndex' should be set to 0 (to indicate destination of server),

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the log File

you are copying from.

the 'genOpServerIP' should be set to the server to which the config will be

saved,

the 'genOpProtocolType' should be set to the IP protocol used to transport

the file.

eraseFile --

The 'genOpDestIndex' Is not applicable for this command,

the 'genOpSourceIndex' should be set to the 'genAppFileId' of the File

you wish to erase.

the 'genOpServerIP' should be set to 0,

the 'genOpProtocolType' should be set to 0.

show --

reporting information to the CLI.

"

::= { genOpEntry 2 }

genOpRunningState OBJECT-TYPE

SYNTAX INTEGER {

idle(1),

beginOperation(2),

waitingIp(3),

runningIp(4),

copyingLocal(5),

readingConfiguration(6),

executing(7)

}

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Identifies the operation to perform and the state of that operation. This

field acts as both the trigger to initiate the operation (via the beginOperation)

and the status field of the operation itself (i.e. waiting-ip, running-ip, etc.).

It is expected that all dependent MIB objects will be set before the trigger is

set to beginOperation. The operations completion is triggered by the return to

the idle state.

idle(1), - Operation not in progress

beginOperation(2), - Trigger by NMS to start the operation

waitingIp(3), - Communication phase; waiting for response

runningIp(4), - Communication phase; transferring data

copyingLocal(5), - Local operation

readingConfiguration(6), - Parsing / Executing configuration file

executing(7) - Executing Command (such as erasing a file or reporting)"

DEFVAL {idle}

::= { genOpEntry 3 }

genOpSourceIndex OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The index value (taken from the genAppFileTable) of the source of the operation.

NOTE: A value of zero (0) here indicates that the Server (specified below) is the

source."

::= { genOpEntry 4 }

genOpDestIndex OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The index value (taken from the genAppFileTable) of the destination of the operation.

NOTE: A value of zero (0) here indicates that the Server (specified below) is the

Destination."

::= { genOpEntry 5 }

genOpServerIP OBJECT-TYPE

SYNTAX IpAddress

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The IP Address of the server from/to which the file has to be Download/Upload.

NOTE: In the case of localPeerTransport this value should be NULL."

::= { genOpEntry 6 }

genOpUserName OBJECT-TYPE

SYNTAX DisplayString (SIZE(0..128))

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Contains the username to be used if the protocol specified in genOpProtocolType

requires one. The default value will be the empty string"

DEFVAL{'0'H}

::= { genOpEntry 7 }

genOpPassword OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..128))

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Contains the password to be used if the protocol specified in genOpProtocolType

requires one. The default value will be the empty string"

DEFVAL{'0'H}

::= { genOpEntry 8 }

genOpProtocolType OBJECT-TYPE

SYNTAX INTEGER {

tftp(1),

ftp(2),

localPeerTransport(3),

localServerTransport(4)

}

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Identifies the protocol between the management station and the device

for Download/Upload of the file."

::= { genOpEntry 9 }

genOpFileName OBJECT-TYPE

SYNTAX DisplayString

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The location (including the FULL path) of the file in the server.

NOTE: In the case of localPeerTransport this value should be NULL."

::= { genOpEntry 10 }

genOpRunningStateDisplay OBJECT-TYPE

SYNTAX DisplayString (SIZE(0..64))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The state of the operation for Display on the terminal during operation process."

```
        ::= { genOpEntry 11 }


    genOpLastFailureIndex OBJECT-TYPE
        SYNTAX INTEGER {
            noError             (1),
            genError            (2),
            configError (3),
            busy (4),
            timeout             (5),
            cancelled           (6),
            incompatibleFile (7),
            fileTooBig          (8),
            protocolError (9),
            flashWriteError (10),
            nvramWriteError (11),
            confFileGenErr (12),
            confFileParseError (13),
            confFileExecError (14),
            undefinedError (100),
            fileNotFound (101),
            accessViolation (102),
            outOfMemory (103),
            illegalOperation (104),
```

unknownTransferId (105),

fileAlreadyExists (106),

noSuchUser (107)

}

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"While a download is in progress this will always be 'no-error'. After a download is complete this indicates the success or failure of the download. If it is anything other than 'no-error' then 'genOpLastFailureDisplay' will contain a textual description of the error. Error codes from 100 upwards are errors returned from a TFTP server. errors below this are locally generated.

Configuration files may return errors after download as a result of reading a config file into the system.

confFileGenErr - General (unknown error)

confFileParseError - Reading of config file resulted in parsing errors.

confFileExecError - Reading of config file resulted in

```
                    execution errors."
        ::= { genOpEntry 12 }

genOpLastFailureDisplay OBJECT-TYPE
        SYNTAX DisplayString (SIZE(0..64))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Contains the last error, Null if there is no error."
        ::= { genOpEntry 13 }

genOpLastWarningDisplay OBJECT-TYPE
        SYNTAX DisplayString (SIZE(0..64))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
       "Last warning which didn't stop the operation (not fatal error)."
        ::= { genOpEntry 14 }

genOpErrorLogIndex OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-write
        STATUS current
```

DESCRIPTION

"The Index in the 'genAppFileTable' under which an error log has been created.

In the case of file that produce errors this file should

contain a log of errors that occurred. (This item should be zero is not exists)"

::= { genOpEntry 15 }

genOpResetSupported OBJECT-TYPE

SYNTAX INTEGER {

supported(1),

notSupported(2)

}

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Indicates if a reset (after operation completion) is supported by this Module."

::= { genOpEntry 16 }

genOpEnableReset OBJECT-TYPE

SYNTAX INTEGER {

enable(1),

disable(2)

}

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Whether to do a reset after the operation completed successfully."

::= { genOpEntry 17 }

genOpNextBootImageIndex OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The row in the 'genAppFileTable' of the default Application that the device

will boot from when a standard reboot is performed."

::= { genOpEntry 18 }

genOpLastBootImageIndex OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The Index in the 'genAppFileTable' of the default Application that the device

was last booted from."

```
        ::= { genOpEntry 19 }


    genOpFileSystemType OBJECT-TYPE

        SYNTAX INTEGER {

            static (1),

            dynamic (2)

            }

        MAX-ACCESS read-only

        STATUS current

        DESCRIPTION

       "Indicates what type of file system is supported by this module.


        A value of 'static' indicates that rows in the 'genAppFileTable'
    are not removable

            nor can new entries be created.


        A value of 'dynamic' indicates that entries in the
    'genAppFileTable' are both

            removable and can be created."

        ::= { genOpEntry 20 }


    genOpReportSpecificFlags OBJECT-TYPE

            SYNTAX INTEGER {

                    fullReport(1),
```

partialReport(2), -- without OSPF database

notSupported(255)

}

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Contain modifiers to the Report operation.

fullReport - Full configuration report

partialReport - A report without the information stored in the OSPF database

notSupported - For operations other than report, this MIB has no meaning and can return not Supported or

not be supported."

::={ genOpEntry 21}

genOpOctetsReceived OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"While a download is in progress this indicates the number

of bytes transferred so far. "

::={ genOpEntry 22}

```
-- The genApplication Group

--

genAppFileTable OBJECT-TYPE

        SYNTAX SEQUENCE OF GenAppFileEntry

        MAX-ACCESS not-accessible

        STATUS current

        DESCRIPTION

       "Table of Application (FILE) entries.  Each row uniquely defines
an

        application in the system.  Applications can be defined as any
entity

       that can be read or written from or to the system.  This includes
software

        images, boot code, configuration files, prom code, etc."

        ::= { genApplications 1 }



genAppFileEntry OBJECT-TYPE

        SYNTAX GenAppFileEntry

        MAX-ACCESS not-accessible

        STATUS current

        DESCRIPTION

        "An entry in the table, containing data about a single
application / config file."

        INDEX  { genOpModuleId, genAppFileId }
```

```
        ::= { genAppFileTable 1 }


GenAppFileEntry  ::=
        SEQUENCE  {
            genAppFileId            Integer32,
            genAppFileName          DisplayString,
            genAppFileType          INTEGER,
            genAppFileDescription   DisplayString,
            genAppFileSize          Integer32,
            genAppFileVersionNumber OCTET STRING,
            genAppFileLocation      INTEGER,
            genAppFileDateStamp     DisplayString,
            genAppFileRowStatus     RowStatus
            }


genAppFileId OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Index which uniquely identifies the application.
      NOTE: This index CANNOT BE ZERO (0) since the index of zero
is reserved as an
```

```
        indication of network server location in the genOpSourceIndex
and genOpDestIndex

        above."

        ::= { genAppFileEntry 1 }


genAppFileName OBJECT-TYPE

        SYNTAX DisplayString (SIZE(0..64))

        MAX-ACCESS read-create

        STATUS current

        DESCRIPTION

        "The name of the application."

        ::= { genAppFileEntry 2 }


genAppFileType OBJECT-TYPE

        SYNTAX INTEGER {

                runningConfiguration(1),

                startupConfiguration(2),

                defaultConfiguration(3),

                report(4),

                genConfigFile(5),

                logFile(6),

                nvramFile(7),

                swRuntimeImage(8),

                swBootImage(9),
```

swComponent(10),

other(11),

swWebImage(12)

}

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The type (class) of the application. This class serves to catagorize the many application

files in the system into some fixed types:

runningConfiguration -- This entry represents a virtual file in the system. Use of this

entry in the genOpTable should serve to cause the system to generate it's configuration

or to force the system to read a new config into it's configuration.

startupConfiguration -- This entry represents a real file that is used at start-up to configure the

device.

defaultConfiguration -- This entry represents a file which contains the default configuration of the

device.

report -- ??

genConfigFile -- This entry represents a file which contains configuration information (similar to the

'startupConfiguration' above but is not automatically read by the device. This entry is used

to represent 'alternate', 'backup' or 'experimental' configurations that the user may which to

store on the device.

nvramFile -- This entry represents a file that is contain in the nvram files system that does not fit

any of the other pre-defined types.

swRuntimeImage -- This entry represents a software images that contains operational code that is

currently being used to run the device.

swBootImage -- This entry represents a software image that contain operational code that is used to

initally boot the device.

swComponent -- This entry represents a file that is stored as an 'alternate', 'backup'

or 'experimental' version of operational code.

other -- other

swWebImage -- The Image file of the embedded Web application (java application, etc)."

::= { genAppFileEntry 3 }

genAppFileDescription OBJECT-TYPE

SYNTAX DisplayString (SIZE(0..64))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"A description of the application."

::= { genAppFileEntry 4 }

genAppFileSize OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The size (expressed as the number of bytes) of the application."

::= { genAppFileEntry 5 }

genAppFileVersionNumber OBJECT-TYPE

SYNTAX OCTET STRING

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The current version of the application. If this files does not carry a version

this field should be NULL."

::= { genAppFileEntry 6 }

genAppFileLocation OBJECT-TYPE

SYNTAX INTEGER {

ram (1),

flashBankA(2),

flashBankB(3),

nvram (4),

bootProm(5)

}

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The physical location of the application."

::= { genAppFileEntry 7 }

genAppFileDateStamp OBJECT-TYPE

SYNTAX DisplayString (SIZE(0..64))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The time stamp is the Real Time if supported otherwise sysUpTime.

The convention for this field is as follows:

Real Time: Entry is prefixed with an 'R' character and time is formatted using the convention for date-and-time (rfc1903)

DISPLAY-HINT 'R-2d-1d-1d,1d:1d:1d.1d,1a1d:1d'

field	octets	contents	range
1	1-2	year	0..65536
2	3	month	1..12
3	4	day	1..31
4	5	hour	0..23
5	6	minutes	0..59
6	7	seconds (use 60 for leap-second)	0..60
7	8	deci-seconds	0..9
8	9	direction from UTC	'+' / '-'
9	10	hours from UTC	0..11
10	11	minutes from UTC	0..59

For example, Tuesday May 26, 1992 at 1:30:15 PM EDT would be

displayed as:

R-1992-5-26,13:30:15.0,-4:0

Note that if only local time is known, then timezone

information (fields 8-10) is not present.

SysUpTime: Entry is prefixed with an 'S' character and time is

formatted using a portion of that date-and-time convention

DISPLAY-HINT 'S-1d-1d,1d:1d:1d.1d'

field	octets	contents	range
1	3	month	1..12
2	4	day	1..31
3	5	hour	0..23
4	6	minutes	0..59
5	7	seconds	0..60
6	8	deci-seconds	0..9

For example,

S-5-26,13:30:15.0

Represents a file that has existed in the system for 5 months, 26 days, 13 hours, 30 minutes, 15 seconds exactly. This value will be reset after a reboot of the system."

::= { genAppFileEntry 8 }

genAppFileRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The status of this entry in the table. Note the available states:

active(1), -- Fully configured and active.

notInService(2) -- NOT SUPPORTED.

notReady(3), -- Entry NOT FULLY configured.

createAndGo(4), -- Used to add new Applications in the system.

createAndWait(5) -- Used to add new Applications in the system.

or destroy(6) -- Used to delete Applications in the system."

::= { genAppFileEntry 9 }

END

D FCC Notice

FCC Notice — Class A Computing Device:

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference. Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference. Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

VCCI Notice — Class A Computing Device:

This equipment is in the Class A category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in commercial and/or industrial areas. Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers. Read the instructions for correct handling.

CE Notice — Class A Computing Device:

Warning!

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Achtung!

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Avertissement!

Cet appareil est un appareil de Classe A. Dans un environnement résidentiel cet appareil peut provoquer des brouillages radioélectriques. Dans ce cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.

Index

Numerics

10/100 port
  auto negotiation speed/duplex advertisement 5-25
10/100 port parameter
  auto-negotiation mode 5-25
  category 5-24
  duplex mode 5-24
  flow control mode 5-24
  name 5-24
  port PACE priority 5-25
  rate limit burst size 5-25
  rate limit mode 5-25
  rate limit rate 5-25
  speed mode 5-24
10Base-T crossover patch cables 2-7
10-port 100BASE-FX 1-14
12-port 10/100BASE-TX 1-14
3Com mapping table
  non-VLAN switch port parameters 5-37
  switch port configuration parameters 5-32
3Com SuperStack, parameters
  automatic VLAN creation 5-38
  port VLAN 5-37
  trunk mode 5-37
  VLAN bindings 5-38
3COM trunked ports 4-9

A

AARP invalid PDU
  AppleTalk global statistics 15-24
AARP reply rx
  AppleTalk global statistics 15-24
AARP reply tx
  AppleTalk global statistics 15-24
AARP req rx
  AppleTalk global statistics 15-24
AARP req tx
  AppleTalk global statistics 15-24
access level
  configuring SNMP communities 2-14
access list
  AppleTalk NBP filter parameters 15-15
  AppleTalk zone filter parameters 15-19
access list name
  IP access list parameters 9-17, 9-18
access list rules
  IP interface 9-15
access lists
  IP interface 9-15
access rule index
  IP access list parameters 9-17, 9-18
access type
  IP access list parameters 9-17, 9-19
Accessing BOOT Mode B-1
active alarm table
  viewing 17-6
active alarms
  checking 17-5
active backpressure 5-24
add IP interface parameters
  admin. state 9-6
  ICMP redirect 9-7
  interface 9-6
  IP routing 9-7
  MAC format 9-6
  mask 9-6
  multicast protocol 9-7
  NetBIOS UDP rebroadcast 9-7
  network address 9-6
  OSPF 9-7
  proxy ARP 9-7
  RIP 9-7
  VLAN 9-6
  VRRP 9-7
adding a user 2-11, 2-13
  password 2-12
  user logins 2-11
  user name 2-12
adding address forward table entries manually 6-12
adding ports to a hunt group 4-28
addr owner override
  VRRP configuration parameters 9-76
address age time

definition 6-1
address forwarding table 6-1
adding entries manually 6-12
capacity 6-8
address forwarding table parameters
group 6-11
index 6-11
MAC address 6-11
persistence 6-12
port 6-11
priority 6-11
status 6-12
TblInst 6-11
valid 6-11
address forwarding table, persistence parameters
ageout 6-14
permanent 6-14
address mask
DVMRP interface statistical parameters 9-60
address table
configuring instance IDs 6-4
address table instance
delete all learned entries 6-7
delete invalid learned entries 6-7
address table instance entry type
learned 6-6
management 6-6
multicast 6-6
self 6-6
address table instance hash table
auto increment 6-7
size 6-7
address table instance parameters
bucket info 6-7
entry type 6-6
entry validity 6-6
hash table 6-7
total number of entries 6-6
VLAN association 6-6
address table sizes
controlling reconfiguration 6-4, 6-8
address table sizing
definition 6-1
address table, age timer
configuring 6-2
address table, super age timer
configuring 6-2
admin
SNMP security level 2-16
admin state
AppleTalk interface parameters 15-6
IPX interface 12-9
admin. state
add IP interface parameters 9-6
IP interface parameters 9-3
adv. address
IRDP parameters 9-79
advertisement
OSPF summaries parameters 11-14
advertisement life time
IRDP parameters 9-80
advertisement timer
VRRP configuration parameters 9-75
advertisements received
VRRP statistical parameters 9-77
advertisements sent
VRRP statistical parameters 9-77
AFT address table 6-3
age
LSA detail 11-27
OSPF link state database parameter 11-26
age interval
Layer 3 cache configuration 18-4
age timer
buffer management table parameters 20-5
aged entries
forwarding cache (FE) parameters 18-11
ageout
address forwarding table, persistence parameters 6-14
persistence entry 6-12
aggregating bandwidth 4-18
aging
Layer 3 cache configuration 18-3
aging interval multiplier
IPX SAP interface parameters 14-2
alarms
log size, setting 17-14
system events, activating 17-14
alarms, event log
definition 17-15
alarms, shutdown log
definition 17-15
all module ports configuration 5-26
all ports configuration, gigabit ports 5-17
allow learning

non-VLAN switch port parameters 5-36
switch port configuration parameters 5-32
always be group membership querier
IGMP interface parameters 9-32
APP1
CPU redundancy configuration 7-10
APP2
CPU redundancy configuration 7-10
AppleTalk
creating an NBP filter 15-13
ethernet versions supported 15-1
event class parameters 17-16
AppleTalk ARP cache table
viewing 15-30, 15-31
AppleTalk ARP cache table statistics
interface 15-31
MAC address 15-31
network range 15-31
node 15-31
TTL 15-31
type 15-31
AppleTalk global routing
enabling 15-3
AppleTalk global statistics
AARP invalid PDU 15-24
AARP reply rx 15-24
AARP reply tx 15-24
AARP req rx 15-24
AARP req tx 15-24
Bcast error 15-24
checksum error 15-24
config addr error 15-25
config zone error 15-25
DDP forward counter 15-24
DDP input counter 15-24
DDP local counter 15-24
DDP output counter 15-24
DDP output long 15-24
DDP output short 15-24
echo reply rx 15-24
echo req rx 15-24
echo req tx 15-24
no client 15-24
no route 15-24
RTMP RDR Rx 15-25
RTMP RDR Tx 15-25
RTMP Rq Rx 15-25
RTMP Rq Tx 15-25
RTMP Rsp Rx 15-25
RTMP Rsp Tx 15-25
Short PDU in error 15-24
too long 15-24
too short 15-24
TTL expired 15-24
viewing 15-23, 15-25
Zip Ext Reply Rx 15-25
Zip Ext Reply Tx 15-25
Zip GNI Rq Rx 15-25
Zip GNI Rq Tx 15-25
Zip GNI Rsp Rx 15-25
Zip GNI Rsp Tx 15-25
Zip Query Rx 15-25
Zip Query Tx 15-25
Zip Reply Rx 15-25
Zip Reply Tx 15-25
AppleTalk interface
deleting 15-9
AppleTalk interface parameters
admin starte 15-6
encapsulation type 15-5
interface 15-5
metric 15-5
network number 15-6
network range end 15-6
network range start 15-6
node 15-6
VLAN 15-5
zone 15-6
AppleTalk interface statistics
interface 15-26
network number 15-26
network range 15-26
node 15-26
seed 15-26
state 15-26
AppleTalk interface, creating 15-3, 15-7
AppleTalk interface, editing 15-7, 15-9
AppleTalk NBP filter
editing 15-16
AppleTalk NBP filter parameters
access list 15-15
interface 15-15
name 15-15
type 15-15
AppleTalk NBP table
viewing 15-34
AppleTalk NBP table parameters
index 15-34

interface 15-34
name 15-34
type 15-34
zone 15-34
AppleTalk overview 15-1
AppleTalk protocols
supported 15-2
AppleTalk route table
viewing 15-27
AppleTalk route table statistics
current number of routes 15-30
interface 15-28
metric 15-28
network range 15-28
next hop 15-28
owner 15-28
peak number of routes 15-30
state 15-28
zones 15-28
AppleTalk route table statistics, viewing 15-29
AppleTalk routing overview 15-1
AppleTalk routing, configuring 15-2
AppleTalk static route
creating 15-10
deleting 15-13
editing 15-12
network number 15-11
network range end 15-11
network range start 15-11
node 15-11
type 15-11
zone 15-11
AppleTalk statistics
viewing 15-22
AppleTalk zone filter
creating 15-18
editing 15-20
AppleTalk zone filter parameters
access list 15-19
interface 15-19
name 15-19
type 15-19
AppleTalk zone table
viewing 15-32
AppleTalk zone table statistics
current number of zones 15-33
index 15-32
name 15-32
network range 15-32
peak number of zones 15-33
AppleTalk zone table statistics, viewing 15-33
application
multicast session client port parameters 16-14
multicast session parameters 16-12
router port display parameters 16-9
area
LSA detail 11-26
OSPF interface parameters 11-7
OSPF summaries parameters 11-14
OSPF virtual link parameters 11-10
area ID
OSPF area parameters 11-5
OSPF link parameters 11-19
OSPF link state database parameter 11-25
OSPF link state database search parameters 11-24
OSPF statistical parameters 11-18
area type
OSPF area parameters 11-5
ARP cache
searching 9-49
ARP cache entries 9-9
ARP cache search parameters
IP address 9-50
VLAN 9-50
AS border route
OSPF global configuration parameters 11-3
AS border Rtrs
OSPF statistical parameters 11-18
ASBR 11-3
Assigning IP Interfaces to the VLAN 9-12
ATM
overview 1-8
attached router ID 1 & 2
LSA detail 11-28
auth key
RIP interface parameters 10-5
VRRP configuration parameters 9-76
auth type
RIP interface parameters 10-5
authentication
OSPF interface parameters 11-8
OSPF virtual link parameters 11-11
authentication failure

event class parameters 17-15
authentication key
OSPF virtual link parameters 11-11
auto increment
address table instance hash table parameter 6-7
auto increment HT size
VLAN configuration parameters 4-5
auto negotiation speed/duplex advertisement
10/100 port 5-25
auto-creation of virtual links
OSPF global configuration parameters 11-3
automatic client pruning
automatic client pruning 16-7
automatic router pruning
automatic router pruning 16-7
automatic session pruning
automatic session pruning 16-7
automatic VLAN creation 4-2, 5-34
3Com SuperStack parameters 5-38
Bay Networks System 5000 parameters 5-38
Cisco Catalyst 5000 parameters 5-37
switch port configuration parameters 5-32
auto-negotiation
Fast Ethernet module 5-22
auto-negotiation mode
10/100 port parameter 5-25

B

bad advertisements received
VRRP statistical parameters 9-77
bad packets received
IPX SAP interface statistical parameters 14-13
RIP statistical parameters 10-8
bad routes received
RIP statistical parameters 10-8
baud rate
console serial port settings 2-19
Bay Networks System 5000, parameters
automatic VLAN creation 5-38
port VLAN 5-38
trunk mode 5-38
VLAN bindings 5-38
Bcast error
AppleTalk global statistics 15-24
BDR address
OSPF link parameters 11-19
BDR choice
OSPF neighbors parameters 11-22
bind to all
Virtual LAN binding options 5-35
bind to received
Virtual LAN binding options 5-35
binding options
Virtual LANs 5-35
binding type
VLAN switch port table parameters 4-6
blocking state (spanning tree bridge port) 4-12
BOOTP relay agent 9-27, 9-28
BOOTP/DHCP in discards
IP routing global statistics 9-45
BOOTP/DHCP in hops exceeded
IP routing global statistics 9-45
BOOTP/DHCP in requests
IP routing global statistics 9-44
BOOTP/DHCP in responses
IP routing global statistics 9-45
BOOTP/DHCP out requests
IP routing global statistics 9-45
BOOTP/DHCP out responses
IP routing global statistics 9-45
BOOTP/DHCP relay agent
IP global configuration parameters 9-9
border Rtrs
OSPF statistical parameters 11-18
bridge forward delay
spanning tree bridge level parameters 4-10
bridge hello time
spanning tree bridge level parameters 4-10
bridge max age
spanning tree bridge level parameters 4-10
bridge port
spanning tree bridge port parameters 4-12
bridge port parameters
bridge port 4-12
designated bridge 4-12
designated cost 4-12
designated port 4-12
designated root 4-12
forward transitions 4-12
name 4-12
port 4-12
state 4-12

bridge ports
configuring 4-11
bridge status
event class parameters 17-16
broadcast packets
Ethernet interface statistical parameters 19-4
bucket info
address table instance parameters 6-7
buffer and queue management,overview 1-27
buffer detailed configuration parameters
memory 20-5
buffer management parameters
fabric port buffers 20-4
physical port buffers 20-4
buffer management table parameters
age timer 20-5
congestion drops 20-6
high and normal overflow drops 20-6
high and normal stale drops 20-6
high priority allocation 20-6
high priority service ratio 20-6
priority threshold 20-6
buffer space 1-28
buffers
managing 20-2, 20-7
bytes
Ethernet interface statistical parameters 19-4

C

CajunDocs CD xxxvii
Cajun-Service-Type required
RADIUS configuration parameters 8-5
category
10/100 port parameter 5-24
gigabit port parameters 5-17
CGMP packet reception statistics
CGMP snooping parameters 16-35
CGMP snooper, configuring/viewing
configuring CGMP snooper 16-34, 16-35
CGMP snooping 16-3
CGMP snooping overview 16-3
CGMP snooping parameters
CGMP packet reception statistics 16-35
enable state 16-35
intelligent multicast session statistics 16-35
checking active alarms 17-5
checksum
IPX datagram fields 12-3
LSA detail 11-27
OSPF link state database parameter 11-26
checksum error
AppleTalk global statistics 15-24
Cisco Catalyst 5000 parameters
port VLAN 5-37
Cisco Catalyst 5000, parameters
automatic VLAN creation 5-37
trunk mode 5-37
VLAN binding 5-37
VTP snooping 5-37
CLI
regaining access 2-24
CLI configuration
supervisor module 2-3
client port 16-2
multicast session parameters 16-12
client pruning timer
client pruning timer 16-7
clients per VLAN, displaying 16-32, 16-34
collisions 19-7
communities
configuring SNMP 2-13, 2-16
SNMP 2-13
Community String 2-14
comparison value
Layer 3 route cache search parameters 18-8
config addr error
AppleTalk global statistics 15-25
config zone error
AppleTalk global statistics 15-25
configuration
event class parameters 17-15
invalid copies 2-32
saving A-2
configuration file management
copy destination 2-31
copy source 2-30
destination filename 2-31
save running configuration to startup configuration 2-30
source filename 2-31
TFTP server IP address 2-31
configuration files 2-27
configuration revision number
VTP snooping parameters 4-33

configure 16-9, 16-10
configure ports
  gigabit module 5-14, 5-18, 5-25
configure source
  port mirroring information parameters 19-9
configure static router ports
  static router ports 16-9, 16-10
configuring
  non-VLAN switch ports 5-36
  switch port 5-30
Configuring a DNS Client 8-1
configuring a DNS client 1-21, 8-1
configuring a Fast Ethernet module 5-19
configuring a redundant CPU 7-8
configuring a redundant element 7-6
configuring all VLAN ports 4-5
configuring an IPX router 12-4, 12-6
configuring AppleTalk routing 15-2
configuring event logs, protocol 17-7, 17-10
Configuring Event Notification 17-16
configuring event notification 17-16
configuring fast start mode 5-39, 5-41
Configuring Fast Start Mode Using the Web Agent 5-39, 5-41
configuring flow control mode
  gigabit module 5-16, 5-22
configuring hunt groups 4-23
configuring IGMP 9-29
configuring IGMP interfaces 9-31
Configuring IGMP Snooping 16-20, 16-21, 16-24
configuring IGMP snooping 16-21, 16-22
configuring IP 9-1
configuring IP global routing 9-8
configuring IP interface access lists 9-15
configuring IP interfaces 9-12
Configuring IP Routing on the Switch 9-11
Configuring IPX Routing Globally 12-4
configuring IPX SAP interfaces 14-1
Configuring LDAP Setting from the Web Agent 9-81, 9-83
configuring multiple interfaces on a VLAN 9-13
configuring physical port parameters
  gigabit ports 5-17
configuring port VLAN parameters 5-33, 5-35
configuring RADIUS client 8-4, 8-5
configuring RIP global configuration 10-1
configuring RMON mirror port 19-8
configuring service port
  gigabit module 5-16, 5-21
configuring the address table age timer 6-2
configuring the address table super age timer 6-2
Configuring the Age Timer and Super Age Timer 6-2
Configuring the Age Timer and Super Age Timer Using the Web Agent 6-2, 6-3
Configuring the IP Interface for the PPP Console 9-86, 9-88
configuring the LGMP server 16-24, 16-27, 16-29
configuring the PPP console static route 9-85
configuring the serial port console
  PPP console 2-21
configuring the supervisor module
  using the CLI 2-3
configuring the temperature system 3-14, 3-15
configuring thresholds 17-2, 17-3, 17-5
configuring user port
  gigabit module 5-16, 5-21
configuring VRRP 9-71
congestion drops
  buffer management table parameters 20-6
connecting a modem 2-20
  overview 2-20
console
  event table actions 17-17
console serial port
  changing 2-17
console serial port settings, changing
  baud rate 2-19
  data bits 2-19
  flow control 2-19
  parity 2-19
  stop bits 2-19
consumer signal
  LDAP statistics 9-84
contacting Lucent xxx
contacting Lucent technical support xxx
controlling address table size reconfiguration 6-4, 6-8
conventions xxxi
cooling system status
  displaying 3-17

copy destination
configuration file management 2-31
copy source
configuration file management 2-30
copying
configuration
invalid combinations 2-32
from the switch or server to a configuration file 2-29
running configuration to startup configuration 2-28, 2-29, 2-32
startup configuration to running configuration 2-29
to a TFTP server 2-29
to the switch 2-29
copying files 2-31
copying from/to a TFTP server 2-31
copying source files 2-29
cost
IP static route parameters 9-25
OSPF interface parameters 11-8
CPU redundancy configuration
APP1 7-10
APP2 7-10
power-up/reset image 7-10
startup config 7-10
status 7-10
CRC alignment errors
Ethernet interface statistical parameters 19-5
creating a BOOTP/DHCP server entry 9-27, 9-28
creating a multinet interface 9-13
creating a static client port 16-18, 16-19
creating a VRRP router 9-74
creating access rules for filtering traffic between subnets 9-22
creating an AppleTalk interface 15-3, 15-7
creating an AppleTalk static route 15-10
creating an AppleTalk zone filter 15-18
creating an IP interface 9-2, 9-8, 9-11
creating an IPX interface 12-7, 12-10
creating an NBP filter
AppleTalk 15-13
creating an VRRP virtual router 9-74, 9-76
Creating Hunt Groups 4-23
creating IP interface access list rules 9-15
creating IPX RIP filters 13-3, 13-7
creating IPX SAP filters 14-4
creating IPX SAP network filters 14-8, 14-12
creating IPX static routes 12-10, 12-12
creating IPX static services 12-14, 12-15
creating OSPF summaries 11-13, 11-14, 11-15
Creating OSPF Summaries Using the Web Agent 11-13
creating OSPF virtual links 11-9, 11-11
creating static ARP entries
IP static route 9-25
Creating Static Client Ports 16-18
creating static IP routes 9-24
Crossbar 1-5, 1-7
crossbar features supported 1-5, 1-7
current entries
forwarding cache (FE) parameters 18-11
current number of routes
AppleTalk route table statistics 15-30
DVMRP routing statistical parameters 9-63
IP routing table statistical parameters 9-49
current number of zones
AppleTalk zone table statistics 15-33
current power available
power system statistical parameters 3-16

D

data bits
console serial port settings 2-19
day
one-time summer time hours configuration 3-11
summer time hours configuration 3-9
DD number
OSPF neighbors parameters 11-21
DDP forward counter
AppleTalk global statistics 15-24
DDP input counter
AppleTalk global statistics 15-24
DDP local counter
AppleTalk global statistics 15-24
DDP output counter
AppleTalk global statistics 15-24
DDP output long
AppleTalk global statistics 15-24
DDP output short
AppleTalk global statistics 15-24
dead interval
OSPF interface parameters 11-8
OSPF virtual link parameters 11-11

debug
protocol event log settings 17-10
default metric
RIP interface parameters 10-4
default password 2-5
default route
RIP interface parameters 10-4
deleting an AppleTalk interface 15-9
deleting an OSPF area 11-6
deleting AppleTalk static routes 15-13
deleting OSPF virtual links 11-12
Deleting Static Client Ports 16-19
deleting static client ports 16-19
Deleting Static Client Ports Using the CLI 16-19
description
event and shutdown log entries 17-12
designated bridge
spanning tree bridge port parameters 4-12
designated cost
spanning tree bridge port parameters 4-12
designated forwarder
DVMRP route table parameters 9-65
designated forwarder(s) table parameters
forwarder cost to source network 9-66
forwarder network address 9-66
forwarding interface 9-66
designated port
spanning tree bridge port parameters 4-12
designated root
spanning tree bridge port parameters 4-12
destination address
Layer 3 route cache search parameters 18-8
destination filename
configuration file management 2-31
destination group address
DVMRP downstream link parameters 9-69
DVMRP multicast forwarding cache parameters 9-68
DVMRP upstream source parameters 9-70
IGMP local multicast forwarding cache parameters 9-57
upstream prune information 9-68
destination network
IPX datagram fields 12-3
destination node
IPX datagram fields 12-3
destination port
Layer 3 route cache search parameters 18-8
destination port number
DVMRP upstream source parameters 9-70
destination socket
IPX datagram fields 12-3
destination subnet
IP access list parameters 9-19
detail link
OSPF link state database parameter 11-25
diagnostics
for switch hardware 7-2
direction
IPX RIP filter parameters 13-4
IPX SAP filter parameters 14-6
IPX SAP network filter parameters 14-9
disabled (spanning tree bridge port) 4-12
disabling 4-15
displaying
intelligent multicasting 16-8
IPX routing global statistics 12-17, 12-19
displaying DVMRP global statistics 9-58
displaying DVMRP multicast forwarding cache 9-67
displaying DVMRP routing table statistics 9-63
displaying frame forwarding cache statistics 18-5, 18-7
displaying global IP routing statistics 9-39, 9-45
displaying IGMP global statistics 9-51
displaying IGMP local multicast forwarding cache 9-56
displaying IPX RIP interface statistics 2-1, 3-1, 5-1, 7-1, 8-1
displaying Layer 3 forwarding cache 18-10
displaying multicast forwarding cache 9-67
Displaying OSPF Links Using the Web Agent 11-19
displaying OSPF neighbors 11-20
displaying OSPF statistics 11-16
displaying router ports 16-8
displaying the cooling system status 3-17
displaying the DVMRP designated forwarder table 9-66
displaying the DVMRP routing table 9-64
Displaying the Forwarding Cache 18-10
displaying the IGMP multicast group table 9-55

displaying the power system statistics 3-15
DNS client
  configuring 1-21, 8-1
document conventions xxxi
documentation
  feedback xxxviii
  online xxxiv
documentation feedback xxxviii
domain name
  VTP snooping parameters 4-33
down state (spanning tree bridge port) 4-12
downloaded image
  viewing A-4
downloading image from TFTP server to an APP location A-3
downstream dependent router
  DVMRP route table parameters 9-65
downstream interface
  DVMRP multicast forwarding cache parameters 9-68
downstream interfaces
  IGMP local multicast forwarding cache parameters 9-57
DR address
  OSPF link parameters 11-19
DR choice
  OSPF neighbors parameters 11-22
DR priority
  OSPF interface parameters 11-7
  OSPF neighbors parameters 11-22
DR router ID
  OSPF link parameters 11-19
DUAL-LAYER SPANNING TREE 1-25
duplex mode
  10/100 port parameter 5-24
duplicate add attempts
  forwarding cache (FE) parameters 18-11
DVMRP
  configuring 9-34
  displaying global statistics 9-58
  modifying information 9-37
DVMRP designated forwarder table
  displaying 9-66
DVMRP downstream dependent router
  DVMRP supported major/minor version 9-67
  found on interface 9-67
  router is SNMP manageable 9-67
  router network address 9-67
  router received probe from this router 9-67
  router supports generation ID function 9-67
  router supports prune function 9-67
DVMRP downstream interface
  DVMRP downstream link parameters 9-69
DVMRP downstream link parameters
  destination group address 9-69
  DVMRP downstream interface 9-69
  interface is pruned 9-70
  interface type 9-70
  prune expiration 9-70
  source subnetwork 9-69
DVMRP downstream routers
  viewing 9-66
DVMRP global statistical parameters
  graft acknowledgments received 9-59
  graft acknowledgments transmitted 9-59
  graft messages received 9-59
  graft messages transmitted 9-59
  probe message received 9-59
  probe messages transmitted 9-59
  prune messages received 9-59
  prune messages transmitted 9-59
  report messages received 9-59
  report messages transmitted 9-59
  unknown messages codes encountered 9-59
DVMRP interface
  modifying 9-37
DVMRP interface parameters
  interface 9-37
  interface metric 9-38
  interface scope 9-38
  interface type 9-38
  IP address 9-37
  IP address mask 9-37
  tunnel endpoint address 9-38
DVMRP interface statistical parameters
  address mask 9-60
  IGMP querier interface 9-61
  interface 9-60
  invalid routes received 9-61
  metric 9-61
  neighbor DVMRP routers 9-61
  network address 9-60
  next probe message in sec 9-61
  state 9-60

type 9-61
unrecognized packets received 9-61
DVMRP interface statistics
examining 9-60
DVMRP multicast forwarding cache
displaying 9-67
DVMRP multicast forwarding cache parameters
destination group address 9-68
downstream interface 9-68
invalid flows from upstream 9-68
next pruned downstream interface to timeout 9-68
packets forwarded through cache entry 9-68
source address mask 9-68
source subnetwork 9-68
upstream interface 9-68
upstream interface is pruned 9-68
upstream neighbor router address 9-68
upstream sources 9-68
DVMRP neighbor routers
DVMRP supported major/minor version 9-62
expiration period 9-62
found on interface 9-62
neighbor is SNMP manageable 9-62
neighbor network address 9-62
neighbor received probe from this router 9-62
neighbor supports generation ID function 9-62
neighbor supports MTRACE requests 9-62
neighbor supports prune function 9-62
viewing 9-61
DVMRP parameters
maximum number of routes 9-36
DVMRP route table parameters
designated forwarder 9-65
downstream dependent router 9-65
expiration period in sec 9-64
reporting router 9-64
reporting router interface 9-64
route metric 9-64
source network 9-64
source network mask 9-64
upstream router 9-65
DVMRP routing statistical parameters
current number of routes 9-63
number of trigger routes 9-63
number of valid routes 9-63
DVMRP routing table
displaying 9-64
DVMRP routing table statistics
displaying 9-63
DVMRP supported major/minor version
DVMRP downstream dependent router 9-67
DVMRP neighbor routers 9-62
DVMRP upstream interface
upstream prune information 9-69
DVMRP upstream routers
found on interface 9-65
router cost to source network 9-65
router network address 9-65
viewing 9-65
DVMRP upstream source parameters
destination group address 9-70
destination port number 9-70
flow source address 9-70
flow upstream interface 9-70
payload protocol type 9-70
source port number 9-70
DVMRP upstream sources 9-70

E

echo reply rx
AppleTalk global statistics 15-24
echo req rx
AppleTalk global statistics 15-24
echo req tx
AppleTalk global statistics 15-24
editing an AppleTalk static route 15-12
editing an AppleTalk zone filter 15-20
editing an NBP filter 15-16
editing AppleTalk interfaces 15-7, 15-9
editing general system information 3-2
egress rules
VLAN 4-3
enable
spanning tree bridge port information parameters 4-13
enable state
CGMP snooping parameters 16-35
enable state 16-7
IGMP snooping 16-21
LGMP client configuration parameters 16-31

LGMP server configuration parameters 16-24
RADIUS configuration parameters 8-5
enabling
enabling IRDP 9-78
enabling AppleTalk global routing 15-3
enabling gigabit ports 5-15, 5-20
enabling SNTP 3-3, 3-4
Enabling the LGMP Server 16-22, 16-23
enabling the rate limit mode
Fast Ethernet module 5-23
enabling VRRP 9-71, 9-73
encapsulation type
AppleTalk interface parameters 15-5
end
one-time summer time hours configuration 3-11
summer time hours configuration 3-8
end network
IPX RIP filter parameters 13-4
entries removed due to route changes
forwarding cache (FE) parameters 18-11
entries removed due to route deletes
forwarding cache (FE) parameters 18-11
entry expiration period in sec
IGMP group membership table parameters 9-56
entry type
address table instance parameters 6-6
entry validity
address table instance parameters 6-6
E-option
OSPF neighbors parameters 11-22
error
protocol event log settings 17-10
Ethernet interface statistical parameters
broadcast packets 19-4
bytes 19-4
CRC alignment errors 19-5
fragments 19-6
interval start 19-4
jabbers 19-7
multicast packets 19-5
oversize packets 19-6
packets 19-4
sample 19-4
undersize packets 19-6
utilization 19-4
Ethernet interface statistics
configuring 19-3
Ethernet statistics, RMON
viewing 19-1, 19-7
event and shutdown log entries
description 17-12
event ID 17-12
log ID 17-12
severity 17-12
time stamp 17-12
type 17-12
event and shutdown logs
viewing 17-11, 17-13
event class parameters
AppleTalk 17-16
authentication failure 17-15
bridge status 17-16
configuration 17-15
fan status 17-15
LDAP 17-16
OSPF 17-16
resource 17-15
RIP 17-16
service port status 17-15
start 17-15
switch fabric 17-16
system 17-15
temperature status 17-15
user port status 17-15
event classes 17-15
event configuration
accessing 17-14, 17-16
event ID
event and shutdown log entries 17-12
event log
definition 17-15
event log (switch event)
definition 17-7
event log wraps
event statistics 17-14
event notification
configuring 17-16
event statistics
event log wraps 17-14
events dropped due to event system queue full 17-14
events dropped due to overload of event system 17-14
viewing 17-13, 17-14, 17-16
event table actions

console 17-17
log 17-17
trap 17-17
events dropped due to event system queue full
event statistics 17-14
events dropped due to overload of event system
event statistics 17-14
examining DVMRP interface statistics 9-60
examining IP routing table statistics 9-48
example of routing with Layer 2/3 1-30
expiration period
DVMRP neighbor routers 9-62
expiration period in sec
DVMRP route table parameters 9-64
Extensive Fault Tolerance 1-27
external
LSA detail 11-27
external LSA count
OSPF statistical parameters 11-17

F

fabric port buffers
buffer management parameters 20-4
failed add attempts
forwarding cache (FE) parameters 18-11
failed element 7-2
fan status
event class parameters 17-15
Fast Ethernet module
auto-negotiation mode, enabling 5-22
configuring 5-19
rate limit mode, enabling 5-23
Fast Ethernet module, configuring
pace priority mode 5-23
rate limit rate 5-23
Fast Ethernet Modules 1-14
fast start
switch port configuration parameters 5-32
fast start mode
configuring 5-39, 5-41
fault
protocol event log settings 17-10
files
copying 2-31
startup.txt 2-27
filter/suppress
IPX RIP filter parameters 13-5
IPX SAP filter parameters 14-6
IPX SAP network filter parameters 14-10
filtering
index 6-11
MAC address 6-11
persistence 6-12
port 6-11
priority 6-11
filtering on the MAC address 6-9
filtering on the VLAN 6-9
filtering traffic between subnets 9-22
FIRE fabric port
frame forwarding statistical parameters 18-6
flow control
console serial port settings 2-19
flow control mode
10/100 port parameter 5-24
gigabit port parameters 5-18
flow source address
DVMRP upstream source parameters 9-70
flow upstream interface
DVMRP upstream source parameters 9-70
forward address
LSA detail 11-27
forward delay
spanning tree bridge level parameters 4-10
forward transitions
spanning tree bridge port parameters 4-12
forwarder cost to source network
designated forwarder(s) table parameters 9-66
forwarder network address
designated forwarder(s) table parameters 9-66
forwarding cache
configuring 18-1, 18-4
displaying 18-10
forwarding cache (FE) parameters
aged entries 18-11
current entries 18-11
duplicate add attempts 18-11
entries removed due to route changes 18-11
entries removed due to route deletes 18-11
failed add attempts 18-11
lookup hits 18-11
lookup levels 18-11
lookup misses 18-11

memory use in bytes 18-11
mode 18-11
PRE 18-11
total entries 18-11
type 18-11
forwarding cache statistics
monitoring 18-5
forwarding interface
designated forwarder(s) table parameters 9-66
Forwarding Rules 5-8
forwarding rules
VLAN 4-2
forwarding state (spanning tree bridge port) 4-12
found on interface
DVMRP downstream dependent router 9-67
DVMRP neighbor routers 9-62
DVMRP upstream routers 9-65
fragments
Ethernet interface statistical parameters 19-6
Frame Classification 1-19
frame format
VLAN switch port table parameters 4-6
frame forwarding cache
displaying statistics 18-5, 18-7
frame forwarding statistical parameters
FIRE fabric port 18-6
L2 frame count 18-6
L3 drop frames 18-6
L3 frame cache hits 18-6
L3 slow path frames 18-6
L3 total (T2) 18-6
percent cache hits 18-6
percent drops 18-6
percent slow path 18-6
RX frame count (T2) 18-6
Frame Tags 5-34
frame tags
switch port configuration parameters 5-31
frame type
IPX interface 12-9
front panel LEDs
HD/FD 17-2
interpreting 17-1
front panel LEDs (10/100 module)
port 17-2
front panel LEDs (gigabit module)
port 17-2

G

general system information, setting
device contact 3-2
device location 3-2
switch name 3-2
get nearest server reply
IPX SAP interface parameters 14-3
get nearest server reply delay
IPX SAP interface parameters 14-3
Gigabit Ethernet modules (L2/L3) 1-14
gigabit module
configure ports 5-14, 5-18, 5-25
gigabit module, configuring
flow control mode 5-16, 5-22
port name 5-15, 5-20
ports 5-15, 5-20
service port 5-16, 5-21
user port 5-16, 5-21
gigabit port name
configuring 5-15, 5-20
gigabit port parameters
category 5-17
flow control mode 5-18
port name 5-17
port PACE priority 5-18
remote fault detect 5-18
gigabit ports
configuring physical port parameters 5-17
enabling 5-15, 5-20
Gigabit-Speed Modules 1-14
global configuration 16-5, 16-8, 16-9
intelligent multicast 16-5, 16-8, 16-9
GLOBAL DISABLE 1-26
global RIP
RIP global configuration parameters 10-2
Globally Enabling VRRP Using the WEeb Agent 9-71
GNS requests received
IPX SAP interface statistical parameters 14-13
GNS responses sent
IPX SAP interface statistical parameters 14-13
graft acknowledgments received
DVMRP global statistical parameters 9-59
graft acknowledgments transmitted

DVMRP global statistical parameters 9-59
graft messages received
DVMRP global statistical parameters 9-59
graft messages transmitted
DVMRP global statistical parameters 9-59
group
address forwarding table parameters 6-11
RADIUS configuration parameters 8-5
group address
IGMP group membership table parameters 9-56
group created on
IGMP group membership table parameters 9-56
group join requests received
IGMP interface statistical parameters 9-54
group leave requests received
IGMP interface statistical parameters 9-54
group member interface
IGMP group membership table parameters 9-56
group membership queries received
IGMP global statistic parameters 9-52
group membership queries transmitted, IGMP global statistic parameters 9-52
group membership reports received
IGMP global statistic parameters 9-52
group multicast protocol
IGMP group membership table parameters 9-56
group reporter address
IGMP group membership table parameters 9-56
group reports received
IGMP interface statistical parameters 9-54

H

hardware requirements for routing 9-11, 12-4
hardware-based routing and bridging 1-13
hash depth
Layer 3 cache configuration 18-3
hash mode
Layer 3 cache configuration 18-3
hash table
address table instance parameters 6-7
HD/FD LED
behavior 17-2
hello interval
OSPF interface parameters 11-8
OSPF virtual link parameters 11-11
hello time
spanning tree bridge level parameters 4-10
Help, Online xxxv
high and normal overflow drops
buffer management table parameters 20-6
high and normal stale drops
buffer management table parameters 20-6
high priority allocation
buffer management table parameters 20-6
high priority service ratio
buffer management table parameters 20-6
high-preference static routes
IP global configuration parameters 9-10
high-priority traffic 20-1
hops
IPX RIP filter parameters 13-5
IPX route table parameter 12-21
IPX SAP filter parameters 14-6
IPX SAP network filter parameters 14-10
IPX service table parameter 12-25
IPX static route 12-12
IPX static service parameter 12-15
hour
one-time summer time hours configuration 3-12
summer time hours configuration 3-9
hunt group
adding ports 4-28
considerations 4-23
non-VLAN switch port parameters 5-36
switch port configuration parameters 5-32
switch port parameter 5-29
hunt group members
viewing details 4-27
hunt groups 1-20
aggregate bandwidth 4-18
before configuring 4-18
configuring 4-23

I

ICMP in address mask reply
IP routing global statistics 9-43
ICMP in address mask requests
IP routing global statistics 9-43
ICMP in destination unreachable
IP routing global statistics 9-43
ICMP in echo replys

IP routing global statistics 9-43
ICMP in echo requests
IP routing global statistics 9-43
ICMP in errors
IP routing global statistics 9-43
ICMP in messages
IP routing global statistics 9-43
ICMP in parameter problems
IP routing global statistics 9-43
ICMP in redirects
IP routing global statistics 9-43
ICMP in source quenches
IP routing global statistics 9-43
ICMP in time exceeds
IP routing global statistics 9-43
ICMP in timestamp replys
IP routing global statistics 9-43
ICMP in timestamp requests
IP routing global statistics 9-43
ICMP out address mask reply
IP routing global statistics 9-44
ICMP out address mask requests
IP routing global statistics 9-44
ICMP out destination unreachable
IP routing global statistics 9-43
ICMP out echo reply
IP routing global statistics 9-44
ICMP out echo requests
IP routing global statistics 9-44
ICMP out errors
IP routing global statistics 9-43
ICMP out messages
IP routing global statistics 9-43
ICMP out parameter problems
IP routing global statistics 9-44
ICMP out redirects
IP routing global statistics 9-44
ICMP out source quenches
IP routing global statistics 9-44
ICMP out time exceeded
IP routing global statistics 9-43
ICMP out timestamp reply
IP routing global statistics 9-44
ICMP out timestamp request
IP routing global statistics 9-44
ICMP redirect
add IP interface parameters 9-7
IP interface parameters 9-3
IEEE 802.3x full duplex flow control,definition 1-13
IEEE 802.3X PAUSE 20-2
IEEE802.1D SPANNING TREE 1-24
IGMP
configuring 9-29
Global statistics 9-51, 9-52, 9-55
overview 9-29
IGMP global statistic parameters
group membership queries received 9-52
group membership queries transmitted 9-52
group membership reports received 9-52
unknown messages received 9-52
IGMP global statistics
displaying 9-51
IGMP group membership table parameters
entry expiration period in sec 9-56
group address 9-56
group created on 9-56
group member interface 9-56
group multicast protocol 9-56
group reporter address 9-56
IGMP interface parameters
always be group membership querier 9-32
IGMP version 9-32
interface 9-32
IP address 9-32
IP address mask 9-32
maximum groups 9-32
neighbor querier timeout interval 9-33
process leave packets 9-32
query request interval 9-32
query response interval 9-33
robustness variable 9-33
IGMP interface statistical parameters
group join requests received 9-54
group leave requests received 9-54
group reports received 9-54
IGMP version 9-54
interface 9-54
IP address 9-54
IP address mask 9-54
neighbor querier timeout in sec 9-54
next query request in sec 9-54
number of current groups 9-55
query messages received 9-54
query messages transmitted 9-54
robustness variable 9-54
state 9-54

this router is group membership querier 9-54
unknown messages received 9-55
IGMP interface statistics
viewing 9-52, 9-55
IGMP interfaces
configuring 9-31
IGMP local multicast forwarding cache
displaying 9-56
IGMP local multicast forwarding cache parameters
destination group address 9-57
downstream interfaces 9-57
invalid flows from upstream 9-57
packets forwarded through cache entry 9-57
source address mask 9-57
source subnetwork 9-57
upstream interface 9-57
upstream source 9-57
IGMP multicast group table
displaying 9-55
IGMP Only Multicast Forwarding 9-29
IGMP querier interface
DVMRP interface statistical parameters 9-61
IGMP snooping 16-3
configuring 16-21, 16-22
IGMP snooping parameters
enable state 16-21
intelligent multicast session statistics 16-21
new client ports added 16-21
new router ports added 16-21
new sessions created 16-21
router ports removed 16-21
sessions destroyed 16-21
IGMP version
IGMP interface parameters 9-32
IGMP interface statistical parameters 9-54
in max hops exceeded
IPX global parameters 12-19
index
address forwarding table parameters 6-11
AppleTalk NBP table parameters 15-34
AppleTalk zone table statistics 15-32
info
protocol event log settings 17-10
ingress rules
VLAN operation 4-2
initial hash table size
VLAN configuration parameters 4-5
installing redundant controllers 7-3
instance IDs
configuring 6-4
intelligent multicast 16-4, 16-17, 16-18, 16-24, 16-27, 16-29, 16-30, 16-32, 16-34, 16-35
session search 16-10, 16-13
intelligent multicast global configuration parameters 16-7
intelligent multicast session statistics
CGMP snooping parameters 16-35
IGMP snooping 16-21
LGMP client configuration parameters 16-31
LGMP client display per VLAN parameters 16-33
LGMP server configuration parameters 16-26
LGMP server display per VLAN parameters 16-29
intelligent multicasting 16-1, 16-3, 16-5, 16-8, 16-9, 16-10
intelligent multicasting 16-3
LGMP client 16-3
interface
add IP interface parameters 9-6
AppleTalk ARP cache table statistics 15-31
AppleTalk interface parameters 15-5
AppleTalk interface statistics 15-26
AppleTalk NBP filter parameters 15-15
AppleTalk NBP table parameters 15-34
AppleTalk route table statistics 15-28
AppleTalk zone filter parameters 15-19
creating a VRRP virtual router 9-74, 9-76
DVMRP interface parameters 9-37
DVMRP interface statistical parameters 9-60
enabling VRRP 9-73
IGMP interface parameters 9-32
IGMP interface statistical parameters 9-54
IP interface parameters 9-3
IP routing table search parameters 9-47
IPX interface 12-9
IPX RIP filter parameters 13-4
IPX route table parameter 12-21
IPX routing table search parameters 12-20
IPX SAP filter parameters 14-5

IPX SAP interface parameters 14-2
IPX SAP interface statistical parameters 14-13
IPX SAP network filter parameters 14-9
IPX service table parameter 12-24
IPX service table search parameter 12-23
IPX static route 12-12
IPX static service parameter 12-15
IRDP parameters 9-79
OSPF interface parameters 11-7
RIP interface parameters 10-3
RIP statistical parameters 10-8
VRRP configuration parameters 9-75
VRRP statistical parameters 9-77
interface is pruned
DVMRP downstream link parameters 9-70
upstream prune information 9-69
interface metric
DVMRP interface parameters 9-38
interface scope
DVMRP interface parameters 9-38
interface type
DVMRP downstream link parameters 9-70
DVMRP interface parameters 9-38
upstream prune information 9-69
interfaces
adding to NBP filter 15-17, 15-18, 15-22
adding to zone filter 15-21, 15-22
deleting from a zone filter 15-21, 15-22
deleting from NBP filter 15-17, 15-18, 15-22
interpreting front panel LEDs 17-1
interpreting IPX SAP interface statistics 14-12, 14-13
interval start
Ethernet interface statistical parameters 19-4
intra-area routes
IP global configuration parameters 9-10
introduction 16-1
invalid entry
permanent, definition 6-12
invalid flows from upstream
DVMRP multicast forwarding cache parameters 9-68
IGMP local multicast forwarding cache parameters 9-57
invalid routes received
DVMRP interface statistical parameters 9-61
IP
creating OSPF summaries 11-13, 11-14, 11-15
creating OSPF virtual links 11-9, 11-11
creating RIP trusted neighbors 10-5, 10-6, 10-7
displaying OSPF links 11-18, 11-19
displaying OSPF neighbors 11-20
displaying OSPF statistics 11-16
DVMRP configuration 9-34
global configuration 9-1
interface configuration 9-12
modifying OSPF areas 11-7
multicast forwarding 9-28
multicast routing 9-28
multicast statistics 9-50
multicast, overview 9-28
OSPF area creation 11-4
OSPF global configuration 11-2
RIP configuring interfaces 10-3
RIP global configuration 10-1
RIP statistics 10-7, 10-8
searching the OSPF link state database 11-23, 11-28
Searching the routing table 9-46
IP access list parameters
access list name 9-17, 9-18
access rule index 9-17, 9-18
access type 9-17, 9-19
destination subnet 9-19
protocol ID 9-19
TCP established 9-20
TCP/UDP destination port 9-20
TCP/UDP source port 9-19
IP access rules
creating rules for filtering traffic between subnets 9-22
filtering traffic between subnets example 9-22
filtering web traffic example 9-21
IP address
ARP cache search parameters 9-50
configuring SNMP communities 2-14
DVMRP interface parameters 9-37
IGMP interface parameters 9-32
IGMP interface statistical parameters 9-54
IP routing table search parameters 9-47
IP static ARP parameters 9-26

OSPF interface parameters 11-7
OSPF link parameters 11-19
OSPF neighbors parameters 11-21
RIP statistical parameters 10-8
static multicast session configuration parameters 16-16
static multicast session parameters 16-17
VRRP configuration parameters 9-75
VRRP statistical parameters 9-77
IP address mask
DVMRP interface parameters 9-37
IGMP interface parameters 9-32
IGMP interface statistical parameters 9-54
IP and IPX router 1-28
IP ARP
searching ARP cache 9-49
IP configuration 9-1
IP forward datagrams
IP routing global statistics 9-41
IP fragmentation creates
IP routing global statistics 9-42
IP fragmentation failures 9-42
IP fragmentation OKs
IP routing global statistics 9-42
IP global configuration parameters
BOOTP/DHCP relay agent 9-9
high-preference static routes 9-10
intra-area routes 9-10
IP multicast forwarding 9-9
IP routing 9-9
IP source routing 9-9
limit proxy ARP to same network 9-9
local routes 9-9
low-preference static routes 9-10
maximum number of ARP cache entries 9-9
maximum number of routes 9-9
OSPF external routes 9-10
OSPF inter-area routes 9-10
RIP routes 9-10
route preference by protocol 9-9
use default route for proxy ARP 9-9
VRRP 9-9
IP global routing
configuring 9-8
IP global routing statistics
displaying 9-39, 9-45
IP in address errors
IP routing global statistics 9-41
IP in delivers
IP routing global statistics 9-41
IP in discards
IP routing global statistics 9-41
IP in header errors
IP routing global statistics 9-41
IP in receives
IP routing global statistics 9-41
IP in unknown protocols
IP routing global statistics 9-41
IP interface
creating 9-2, 9-8, 9-11
IP interface access list rules
creating 9-15
IP interface access lists
configuring 9-15
IP interface parameters
admin. state 9-3
ICMP redirect 9-3
interface 9-3
IP routing 9-3
MAC format 9-3
mask 9-3
multicast protocol 9-3
NetBIOS UDP rebroadcast 9-4
network address 9-3
OSPF 9-3
proxy ARP 9-3
RIP 9-3
state 9-3
VLAN 9-3
VRRP 9-4
IP interfaces
configuring 9-12
IP multicast
overview 9-28
IP multicast forward datagrams
IP routing global statistics 9-44
IP multicast forwarding
IP global configuration parameters 9-9
IP multicast in discard
IP routing global statistics 9-44
IP multicast in receives
IP routing global statistics 9-44
IP out discards
9-42
IP out no routes
IP routing global statistics 9-42
IP out requests

IP routing global statistics 9-42
IP reassembly failures
IP routing global statistics 9-42
IP reassembly OKs
IP routing global statistics 9-42
IP reassembly required
IP routing global statistics 9-42
IP reassembly timeout
IP routing global statistics 9-42
IP routing
add IP interface parameters 9-7
creating a BOOTP/DHCP server entry 9-27, 9-28
IP global configuration parameters 9-9
IP interface parameters 9-3
statistics 9-38
IP routing discards
IP routing global statistics 9-42
IP routing global statistics
BOOTP/DHCP in discards 9-45
BOOTP/DHCP in hops exceeded 9-45
BOOTP/DHCP in requests 9-44
BOOTP/DHCP in responses 9-45
BOOTP/DHCP out requests 9-45
BOOTP/DHCP out responses 9-45
ICMP in address mask reply 9-43
ICMP in address mask requests 9-43
ICMP in destination unreachable 9-43
ICMP in echo replys 9-43
ICMP in echo requests 9-43
ICMP in errors 9-43
ICMP in messages 9-43
ICMP in parameter problems 9-43
ICMP in redirects 9-43
ICMP in source quenches 9-43
ICMP in time exceeds 9-43
ICMP in timestamp replys 9-43
ICMP in timestamp requests 9-43
ICMP out address mask reply 9-44
ICMP out address mask requests 9-44
ICMP out destination unreachable 9-43
ICMP out echo reply 9-44
ICMP out echo requests 9-44
ICMP out errors 9-43
ICMP out messages 9-43
ICMP out parameter problems 9-44
ICMP out redirects 9-44
ICMP out source quenches 9-44
ICMP out time exceeded 9-43
ICMP out timestamp reply 9-44
ICMP out timestamp request 9-44
IP forward datagrams 9-41
IP fragmentation creates 9-42
IP fragmentation failures 9-42
IP fragmentation OKs 9-42
IP in address errors 9-41
IP in delivers 9-41
IP in discards 9-41
IP in header errors 9-41
IP in receives 9-41
IP in unknown protocols 9-41
IP multicast forward datagrams 9-44
IP multicast in discard 9-44
IP multicast in receives 9-44
IP out discards 9-42
IP out no routes 9-42
IP out requests 9-42
IP reassembly failures 9-42
IP reassembly OKs 9-42
IP reassembly required 9-42
IP reassembly timeout 9-42
IP routing discards 9-42
UDP in datagrams 9-44
UDP in errors 9-44
UDP in no ports 9-44
UDP out datagrams 9-44
IP routing search table
deleting local entries from routing table 9-48
IP routing statistics 9-38
IP routing table
searching 9-46
IP routing table search parameters
interface 9-47
IP address 9-47
source 9-47
IP routing table statistical parameters
current number of routes 9-49
peak number of routes 9-49
RIP queries 9-49
RIP route changes 9-49
total routes added 9-49
total routes deleted 9-49
IP routing table statistics
examining 9-48
IP source routing
IP global configuration parameters 9-9
IP static ARP parameters

IP address 9-26
MAC address 9-26
IP static route
creating static ARP entries 9-25
IP static route parameters
cost 9-25
mask 9-25
network address 9-25
next-hop address 9-25
next-hop VLAN 9-25
preference 9-25
IP static routes
creating 9-24
IPX C-1
creating static routes 12-10, 12-12
creating static services 12-14, 12-15
datagram structure 12-2
deleting static routes 12-12, 12-13
deleting static service 12-16, 12-17
examining the route table 12-21
examining the service table 12-24
global statistics 12-17, 12-19
interface configuration 12-7, 12-10
modifying IPX RIP filters 13-3, 13-7
modifying static routes 12-13
modifying static services 12-16
network number 12-1
node number 12-1
RIP interfaces 13-1
routing table statistics 12-22
searching the route table 12-19
searching the service table 12-22
socket number 12-1
IPX datagram fields
checksum 12-3
destination network 12-3
destination node 12-3
destination socket 12-3
packet length 12-3
packet type 12-3
source network 12-3
source node 12-3
source socket 12-3
transport control 12-3
IPX datagram structure 12-2
IPX forward datagrams
IPX global parameters 12-18
IPX global parameters 12-6, 12-10
in max hops exceeded 12-19
IPX forward datagrams 12-18
IPX in checksum errors 12-19
IPX in delivery 12-18
IPX in discards 12-18
IPX in header errors 12-18
IPX in ping replies 12-19
IPX in ping request 12-19
IPX in receives 12-18
IPX in unknown sockets 12-19
IPX Netbios receives 12-18
IPX out discards 12-19
IPX out no routes 12-19
IPX out packets 12-19
IPX out ping replies 12-19
IPX out ping requests 12-19
IPX out requests 12-19
maximum number of services 12-6
IPX in checksum errors
IPX global parameters 12-19
IPX in delivery
IPX global parameters 12-18
IPX in discards
IPX global parameters 12-18
IPX in header errors
IPX global parameters 12-18
IPX in ping replies
IPX global parameters 12-19
IPX in ping request
IPX global parameters 12-19
IPX in receives
IPX global parameters 12-18
IPX in unknown sockets
IPX global parameters 12-19
IPX interface
admin state 12-9
frame type 12-9
interface 12-9
network address 12-9
node address 12-9
RIP 12-9
state 12-9
ticks 12-9
type 20 packet propagation 12-10
VLAN 12-9
IPX interface MIbs C-1
IPX interface parameters 12-9
IPX Netbios receives
IPX global parameters 12-18
IPX out discards

IPX global parameters 12-19
IPX out no routes
IPX global parameters 12-19
IPX out packets
IPX global parameters 12-19
IPX out ping replies
IPX global parameters 12-19
IPX out pint requests
IPX global parameters 12-19
IPX out requests
IPX global parameters 12-19
IPX overview 12-1
IPX RIP filter
suppress advertising of all networks example 13-5, 13-6
IPX RIP filter parameters
direction 13-4
end network 13-4
filter/suppress 13-5
hops 13-5
interface 13-4
precedence 13-4
start network 13-4
ticks 13-5
IPX RIP filters
creating 13-3, 13-7
IPX RIP filters, modifying 13-3, 13-7
IPX RIP interface statistics
displaying 2-1, 3-1, 5-1, 7-1, 8-1
IPX route table
examining 12-21
IPX route table parameters
hops 12-21
interface 12-21
network 12-21
next-hop MAC address 12-21
source 12-21
ticks 12-21
TTL 12-21
IPX route table search 12-19
IPX route table statistics
examining 12-22
IPX router
configuring 12-4, 12-6
IPX routing
IPX routing 12-6
IPX routing global statistics, displaying 12-17, 12-19
IPX routing table search parameters
interface 12-20
network number 12-20
source 12-20
IPX routing table statistics
current number of routes 12-22
peak number of routes 12-22
route add failures 12-22
IPX SAP filter parameters
direction 14-6
filter/suppress 14-6
hops 14-6
interface 14-5
name 14-5
precedence 14-5
type 14-6
IPX SAP filters
creating 14-4
filtering all services except NDS example 14-10
suppress advertising of print servers example 14-7
IPX SAP interface parameters
aging interval multiplier 14-2
get nearest server reply 14-3
get nearest server reply delay 14-3
interface 14-2
mode 14-3
network number 14-2
periodic update interval 14-2
triggered updates 14-3
use interpacket gap 14-2
use max packet size 14-2
IPX SAP interface statistical parameters
bad packets received 14-13
GNS requests received 14-13
GNS responses sent 14-13
interface 14-13
network number 14-13
non-triggered updates sent 14-13
requests received 14-13
state 14-13
updates received 14-13
IPX SAp interface statistical parameters
triggered updates sent 14-13
IPX SAP interface statistics
interpreting 14-12, 14-13
IPX SAP interfaces
configuring 14-1
IPX SAP network filter parameters

direction 14-9
filter/suppress 14-10
hops 14-10
interface 14-9
net 14-9
precedence 14-9
type 14-9
IPX SAP network filters
creating 14-8, 14-12
IPX service table
examining 12-24
searching 12-22
IPX service table parameter
hops 12-25
interface 12-24
network 12-24
next-hop MAC address 12-25
node 12-24
socket 12-24
source 12-25
TTL 12-25
type 12-24
IPX service table parameters
name 12-24
IPX service table search parameter
service name 12-23
service type 12-23
IPX service table search parameters
interface 12-23
source 12-23
IPX static route
hops 12-12
interface 12-12
network 12-12
next-hop node 12-12
ticks 12-12
IPX static route parameters 12-12
IPX static routes
creating 12-10, 12-12
deleting 12-12, 12-13
modifying 12-13
IPX static service parameter
hops 12-15
interface 12-15
network 12-15
next-hop node 12-15
node 12-15
service name 12-15
socket 12-15
type 12-15
IPX static service parameters 12-15
IPX static services
creating 12-14, 12-15
IPX syntax example 12-1
IRDP 9-78
enabling on an interface 9-78
IRDP overview 9-78
IRDP parameters
adv. address 9-79
advertisement life time 9-80
interface 9-79
IRDP state 9-79
max. advertisement interval 9-80
minimum advertisement interval 9-79
network address 9-79
preferences 9-79
IRDP state
IRDP parameters 9-79

J

jabbers
Ethernet interface statistical parameters 19-7

K

key
OSPF interface parameters 11-8
known mode
non-VLAN switch port parameters 5-37
switch port configuration parameters 5-32

L

L2 frame count
frame forwarding statistical parameters 18-6
L3 drop frames
frame forwarding statistical parameters 18-6
L3 frame cache hits
frame forwarding statistical parameters 18-6
L3 slow path frames
frame forwarding statistical parameters 18-6
L3 total (T2)
frame forwarding statistical parameters 18-6
LAN router

configuration 9-12
last change
LDAP statistics 9-84
Layer 2 16-3
event log 17-7
redundant switch matrix and controller module 1-27
shutdown log 17-7
Layer 2 Fast Ethernet modules
20-port 10/100BASE-TX 1-14
Layer 2 Gigabit Ethernet modules 1-14
Layer 2 overview 16-3
Layer 2 routing
overview 1-29
layer 2 Supervisor module features 1-9
Layer 2 switching 1-28
Layer 2 switching (bridging) 9-11
Layer 2/3 routing example 1-30
Layer 3 (learned) traffic routing
overview 1-29
Layer 3 (not learned) traffic routing
overview 1-29
Layer 3 cache configuration
age interval 18-4
aging 18-3
hash depth 18-3
hash mode 18-3
maximum entries 18-4
Layer 3 dynamic intelligent multicasting 16-2
Layer 3 forwarding cache
displaying 18-10
Layer 3 forwarding cache (FE) parameters
aged entries 18-11
current entries 18-11
duplicate add attempts 18-11
entries removed due to route changes 18-11
entries removed due to route deletes 18-11
failed add attempts 18-11
lookup hits 18-11
lookup levels 18-11
lookup misses 18-11
memory use in bytes 18-11
mode 18-11
PRE 18-11
total entries 18-11
type 18-11
Layer 3 intelligent multicasting
intelligent multicasting 16-3
Layer 3 overview 16-2
Layer 3 route cache search parameters
comparison value 18-8
destination address 18-8
destination port 18-8
PRE 18-9
protocol 18-8
rule number 18-9
source address 18-8
source port 18-8
VLAN 18-8
Layer 3 routing
overview 1-29
Layer 3 switching (routing) 9-11
LDAP
configuring 9-81
configuring settings 9-81, 9-83
configuring statistics 9-83, 9-85
event class parameters 17-16
settings 9-81
LDAP configuration parameters
primary server IP address 9-82
primary server port 9-82
search base 9-83
secondary server IP address 9-82
secondary server port 9-83
LDAP statistics
consumer signal 9-84
last change 9-84
producer signal 9-84
learned entries
delete invalid learned entries 6-7
learning state (spanning tree bridge port) 4-12
LEDs
HD/FD 17-2
port (10/100 module) 17-2
port (gigabit module) 17-2
LGMP client 16-3
LGMP client configuration parameters
enable state 16-31
intelligent multicast session statistics 16-31
LGMP clients 16-31
LGMP message reception statistics 16-31
LGMP client display per VLAN parameters
intelligent multicast session statistics 16-33
LGMP message reception statistics 16-33
VLAN 16-33

LGMP client, configuring
configuring/viewing a LGMP client 16-30, 16-32
LGMP clients
LGMP client configuration parameters 16-31
LGMP message reception statistics
LGMP client configuration parameters 16-31
LGMP client display per VLAN parameters 16-33
LGMP server display per VLAN parameters 16-28
LGMP message statistics
LGMP server configuration parameters 16-25
LGMP message transmission statistics
LGMP server configuration parameters 16-26
LGMP messages transmission statistics
LGMP server display per VLAN parameters 16-29
LGMP server 16-3
LGMP server configuration 16-24, 16-27, 16-29
LGMP server configuration parameters
enable state 16-24
intelligent multicast session statistics 16-26
LGMP message reception statistics 16-25
LGMP message transmission statistics 16-26
LGMP servers 16-25
proxy mode 16-24
robustness variable 16-25
router report time 16-25
server ID priority 16-25
LGMP server display per VLAN parameters
intelligent multicast session statistics 16-29
LGMP message reception statistics 16-28
LGMP messages transmission statistics 16-29
state 16-28
VLAN 16-28
LGMP servers
LGMP server configuration parameters 16-25
limit proxy ARP to same network
IP global configuration parameters 9-9
link data
LSA detail 11-27
link ID
LSA detail 11-27
link state database 11-23, 11-28
link state database search parameters
area ID 11-24
router ID 11-24
type 11-24
links
switch port parameter 5-29
listening state (spanning tree bridge port) 4-12
load MIB
overview 1-23, C-4
local ext type
OSPF global configuration parameters 11-3
local routes
IP global configuration parameters 9-9
log
event table actions 17-17
log ID
event and shutdown log entries 17-12
logging into
Web Agent 2-8
lookup hits
forwarding cache (FE) parameters 18-11
lookup levels
forwarding cache (FE) parameters 18-11
lookup misses
forwarding cache (FE) parameters 18-11
low shutdown temperature
temperature threshold parameter 17-4
lower warning temperature
temperature threshold parameter 17-4
low-preference static routes
IP global configuration parameters 9-10
LS ID
LSA detail 11-27
OSPF link state database parameter 11-25
LSA checksum sum
OSPF statistical parameters 11-17
LSA chksum sum
OSPF statistical parameters 11-18
LSA detail
age 11-27
area 11-26
attached router ID 1 & 2 11-28
checksum 11-27

external 11-27
forward address 11-27
link data 11-27
link ID 11-27
LS ID 11-27
metric 11-27
network mask 11-27
router ID 11-27
sequence 11-27
tag 11-28
TOS 11-27
TOS 0 metric 11-27
TOS count 11-27
type 11-26
type (network) 11-27
LSAs
OSPF statistical parameters 11-18

M

MAC Address
search 6-9
MAC address
address forwarding table parameters 6-11
AppleTalk ARP cache table statistics 15-31
filtering 6-9
IP static ARP parameters 9-26
multicast session parameters 16-12
static multicast session configuration parameters 16-16
static multicast session parameters 16-17
switch port parameter 5-29
MAC address value
adding 6-13
MAC format
add IP interface parameters 9-6
IP interface parameters 9-3
managing buffers and queues 20-2, 20-7
mask
add IP interface parameters 9-6
IP interface parameters 9-3
IP static route parameters 9-25
OSPF summaries parameters 11-14
master
OSPF neighbors parameters 11-21
max age
spanning tree bridge level parameters 4-10
max packets per second
port mirroring information parameters 19-9
max. packets per secondl
mirror port configuration parameters 19-12
max.advertisement interval
IRDP parameters 9-80
maximum entries
Layer 3 cache configuration 18-4
maximum groups
IGMP interface parameters 9-32
maximum number of ARP cache entries
IP global configuration parameters 9-9
maximum number of paths
OSPF global configuration parameters 11-3
maximum number of routes
DVMRP parameters 9-36
IP global configuration parameters 9-9
maximum number of routes 12-6
maximum number of services
IPX global parameters 12-6
MC-option
OSPF neighbors parameters 11-22
MD5 key ID
OSPF interface parameters 11-8
OSPF virtual link parameters 11-11
memory
buffer detailed configuration parameters 20-5
memory use in bytes
forwarding cache (FE) parameters 18-11
metric
AppleTalk interface parameters 15-5
AppleTalk route table statistics 15-28
DVMRP interface statistical parameters 9-61
LSA detail 11-27
MIB groups supported C-1
MIBs
AppleTalk C-4
bridge MIBs C-2
DVMRP C-4
IEEE 802.3 MAU C-2
IEEE 802.3 statistics group C-2
IGMP C-3
IP access list C-4
IP forwarding/routing table C-4
IP interface C-3
IP version 4.0 C-3
OSPF v2.0 C-2

policy capability MIB for LDAP C-4
private IPX interface MIBs C-1
Prominent C-1
RIP v1 and v2 C-2
RMON C-2
SNMPv2 C-2
VRRP C-3
minimum adv. interval
IRDP parameters 9-79
minutes
one-time summer time hours configuration 3-12
summer time hours configuration 3-9
mirror port
configuring
configuring a mirror port 19-8, 19-12
port mirroring information parameters 19-9
RMON mirror port configuration parameters 19-10
switch port configuration parameters 5-32
mirror port configuration parameters
max. packets per second 19-12
mirror port name
port mirroring information parameters 19-9
mode
forwarding cache (FE) parameters 18-11
IPX SAP interface parameters 14-3
RIP interface parameters 10-4
spanning tree bridge level parameters 4-10
modem
connecting 2-20
modem configuration string parameters
&D0 2-22
CD follows carrier 2-22
E0 2-22
S0=1 2-22
software flow control 2-22
modify IPX static routes 12-13
modifying DVMRP interface information 9-37
modifying IGMP interfaces 9-31
Modifying OSPF Interfaces 11-7
Modifying OSPF Summaries 11-15
modifying OSPF virtual links 11-12, 11-13
module features 1-13
module status LED
definition 17-1
modules & ports 4-31, 5-14, 5-19, 5-26, 5-28, 5-30, 5-39, 5-41
monitoring switch performance
IP routing statistics 9-38
OSPF 11-16
Monitoring the Forwarding Cache Statistics 18-5
month
one-time summer time hours configuration 3-11
summer time hours configuration 3-9
multicast forwarding
description 9-28
multicast forwarding cache
displaying 9-67
multicast packets
Ethernet interface statistical parameters 19-5
multicast protocol
add IP interface parameters 9-7
IP interface parameters 9-3
multicast routing
description 9-28
multicast session 16-1
multicast session client port parameters
application 16-14
port 16-14
multicast session parameters
application 16-12
client port 16-12
MAC address 16-12
session ID 16-12
type 16-12
VLAN 16-12
multicast statistics
IP 9-50
multi-gigabit connections example 4-18
multilayer Fast Ethernet modules
20-port 10/100BASE-TX 1-14
multi-link trunk groups
features 4-18
multinetting 9-13, 12-7

N

name
AppleTalk NBP filter parameters 15-15
AppleTalk NBP table parameters 15-34
AppleTalk zone filter parameters 15-19
AppleTalk zone table statistics 15-32

IPX SAP filter parameters 14-5
IPX service table parameter 12-24
spanning tree bridge port parameters 4-12
switch port parameter 5-29
NBP filter
adding interfaces 15-17, 15-18, 15-22
deleting interfaces 15-17, 15-18, 15-22
editing 15-16
neighbor DVMRP routers
DVMRP interface statistical parameters 9-61
neighbor is SNMP manageable
DVMRP neighbor routers 9-62
neighbor network address
DVMRP neighbor routers 9-62
neighbor querier timeout in sec
IGMP interface statistical parameters 9-54
neighbor querier timeout interval
IGMP interface parameters 9-33
neighbor received probe from this router
DVMRP neighbor routers 9-62
neighbor supports generation ID function
DVMRP neighbor routers 9-62
neighbor supports MTRACE requests
DVMRP neighbor routers 9-62
neighbor supports prune function
DVMRP neighbor routers 9-62
net
IPX SAP network filter parameters 14-9
NetBIOS UDP rebroadcast
add IP interface parameters 9-7
IP interface parameters 9-4
network
IPX route table parameter 12-21
IPX service table parameter 12-24
IPX static route 12-12
IPX static service parameter 12-15
network address
add IP interface parameters 9-6
DVMRP interface statistical parameters 9-60
IP interface parameters 9-3
IP static route parameters 9-25
IPX interface 12-9
IRDP parameters 9-79
OSPF summaries parameters 11-14
RIP interface parameters 10-3
network mask
LSA detail 11-27
network number
AppleTalk interface parameters 15-6
AppleTalk interface statistics 15-26
AppleTalk static route 15-11
IPX routing table search parameters 12-20
IPX SAP interface parameters 14-2
IPX SAP interface statistical parameters 14-13
network range
AppleTalk ARP cache table statistics 15-31
AppleTalk interface statistics 15-26
AppleTalk route table statistics 15-28
AppleTalk zone table statistics 15-32
network range end
AppleTalk interface parameters 15-6
AppleTalk static route 15-11
network range start
AppleTalk interface parameters 15-6
AppleTalk static route 15-11
new client ports added
IGMP snooping 16-21
new router ports added
IGMP snooping 16-21
new sessions created
IGMP snooping 16-21
next hop
AppleTalk route table statistics 15-28
next probe message in sec
DVMRP interface statistical parameters 9-61
next pruned downstream interface to time-out
DVMRP multicast forwarding cache parameters 9-68
next query request in sec
IGMP interface statistical parameters 9-54
next-hop address
IP static route parameters 9-25
next-hop MAC address
IPX route table parameter 12-21
IPX service table parameter 12-25
next-hop node
IPX static route 12-12
IPX static service parameter 12-15
next-hop VLAN
IP static route parameters 9-25
no client
AppleTalk global statistics 15-24
no route

AppleTalk global statistics 15-24
node
AppleTalk ARP cache table statistics 15-31
AppleTalk interface parameters 15-6
AppleTalk interface statistics 15-26
AppleTalk static route 15-11
IPX service table parameter 12-24
IPX static service parameter 12-15
node address
IPX interface 12-9
none
SNMP access level 2-15
non-tagged access mode,definition 1-13
non-triggered updates sent
IPX SAP interface statistical parameters 14-13
RIP statistical parameters 10-8
non-VLAN switch port
configuring 5-36
non-VLAN switch port parameters, configuring
3Com mapping table 5-37
allow learning 5-36
hunt group 5-36
known mode 5-37
spanning tree 5-36
N-option
OSPF neighbors parameters 11-22
normal
SNMP security level 2-16
normal-priority traffic 20-1
number of current groups
IGMP interface statistical parameters 9-55
number of routes
IPX routing table statistic 12-22
number of triggered routes
DVMRP routing statistical parameters 9-63
number of valid routes
DVMRP routing statistical parameters 9-63

O

one-time summer time hours configuration 3-11
day 3-11
end 3-11
hour 3-12
minutes 3-12
month 3-11
start 3-11
week 3-11
Online documentation
adding files to a Web server xxxvi
getting updated online documentation xxxvii
installing xxxv
installing the HTTP server xxxv
starting the HTTP server xxxv
online documentation xxxiv
Online Help xxxiv
Online help xxxv
accessing help files from the server xxxvi
adding files to a Web server xxxvi
getting updated help files xxxvii
Open Trunk technology features 1-21
OpenTrunk technology,overview 1-20
OPQ option
OSPF neighbors parameters 11-22
originate LSA count
OSPF statistical parameters 11-17
OSPF
add IP interface parameters 9-7
creating areas 11-4
creating summaries 11-13, 11-14, 11-15
creating virtual links 11-9, 11-11
displaying links 11-18, 11-19
displaying neighbors 11-20
event class parameters 17-16
IP interface parameters 9-3
monitoring switch performance 11-16
OSPF global configuration parameters 11-3
searching the link state database 11-23, 11-28
OSPF area parameters
area ID 11-5
area type 11-5
stub metric 11-5
translate 7 into 5 11-5
type 3 ASE filter 11-5
OSPF areas
deleting 11-6
OSPF external routes
IP global configuration parameters 9-10
OSPF global configuration
configuring 11-2
OSPF global configuration parameters
AS border route 11-3
auto-creation of virtual links 11-3

local ext type 11-3
maximum number of paths 11-3
OSPF 11-3
RIP ext type 11-3
router ID 11-3
SPF hold time 11-3
SPF suspend 11-3
static ext type 11-3
static low ext type 11-3
OSPF inter-area routes
IP global configuration parameters 9-10
OSPF interface parameters
area 11-7
authentication 11-8
cost 11-8
dead interval 11-8
DR priority 11-7
hello interval 11-8
interface 11-7
IP address 11-7
key 11-8
MD5 key ID 11-8
poll interval 11-8
retransmit interval 11-8
transit delay 11-7
OSPF interfaces
modifying 11-7
OSPF link parameters
area ID 11-19
BDR address 11-19
DR address 11-19
DR router ID 11-19
IP address 11-19
state 11-19
type 11-19
OSPF link state database parameter
age 11-26
area ID 11-25
checksum 11-26
detail link 11-25
LS ID 11-25
router ID 11-26
sequence 11-26
type 11-25
OSPF link state database search parameters
area ID 11-24
router ID 11-24
type 11-24
OSPF neighbors parameters
BDR choice 11-22
DD number 11-21
DR choice 11-22
DR priority 11-22
E-option 11-22
IP address 11-21
master 11-21
MC-option 11-22
N-option 11-22
OPQ-option 11-22
router ID 11-21
state 11-21
T-option 11-22
OSPF packet tracing
enabling 17-7, 17-10
OSPF state
OSPF statistical parameters 11-17
OSPF statistical parameters
area ID 11-18
AS border Rtrs 11-18
border Rtrs 11-18
external LSA count 11-17
LSA checksum sum 11-17
LSA chksum sum 11-18
LSAs 11-18
originate LSA count 11-17
OSPF state 11-17
OSPF version 11-17
receive new LSA count 11-17
router ID 11-17
SPF runs 11-18
OSPF statistics
displaying 11-16
OSPF summaries parameters
advertisement 11-14
area 11-14
mask 11-14
network address 11-14
OSPF version
OSPF statistical parameters 11-17
OSPF virtual link parameters
area 11-10
authentication 11-11
authentication key 11-11
dead interval 11-11
hello interval 11-11
MD5 key ID 11-11
retransmit interval 11-10
router ID 11-10

transit delay 11-10
OSPF virtual links
deleting 11-12
modifying 11-12, 11-13
overflow drops
buffer management table parameters 20-6
oversize packets
Ethernet interface statistical parameters 19-6
overview 1-20
ATM 1-8
intelligent multicasting 16-2
Layer 2 16-3
overview of Layer 2 traffic routing 1-29
overview of Layer 3 (learned) traffic routing 1-29
overview of Layer 3 (not learned) traffic routing 1-29
overview of Layer 3 routing 1-29
owner
AppleTalk route table statistics 15-28

P

packet length
IPX datagram fields 12-3
packet tracing
enabling 17-7, 17-10
packet type
IPX datagram fields 12-3
packets
Ethernet interface statistical parameters 19-4
packets forwarded through cache entry
DVMRP multicast forwarding cache parameters 9-68
IGMP local multicast forwarding cache parameters 9-57
parity
console serial port settings 2-19
path cost
spanning tree bridge port information parameters 4-14
payload protocol type
DVMRP upstream source parameters 9-70
peak number of routes
AppleTalk route table statistics 15-30
IP routing table statistical parameters 9-49
IPX routing table statistic 12-22
peak number of zones
AppleTalk zone table statistics 15-33
PER VLAN SPANNING TREE 1-24
percent cache hits
frame forwarding statistical parameters 18-6
percent drops
frame forwarding statistical parameters 18-6
percent slow path
frame forwarding statistical parameters 18-6
performing a system reset 3-18
periodic update interval
IPX SAP interface parameters 14-2
permanent
address forwarding table, persistence parameters 6-14
invalid entry 6-12
persistence entry 6-12
persistence
address forwarding table parameters 6-12
persistence entry
ageout, definition 6-12
permanent, definition 6-12
physical port buffers
buffer management parameters 20-4
piggyback port
port mirroring information parameters 19-9
port mirroring parameter 19-11
poll interval
OSPF interface parameters 11-8
port
address forwarding table parameters 6-11
multicast session client port parameters 16-14
RMON mirror port configuration parameters 19-10
router port display parameters 16-9
spanning tree bridge port parameters 4-12
switch port parameter 5-29
VLAN switch port table parameters 4-6
port density 1-4, 1-6, 1-7
port LED (10/100 module)
behavior 17-2
port LED (gigabit module)
behavior 17-2
port mirror 19-8
port mirroring information parameters 19-9

configure source 19-9
max packets per second 19-9
mirror port 19-9
mirror port name 19-9
piggyback port 19-9
sampler type 19-9
source port 19-9
port mirroring parameters 19-12
port name
gigabit port parameters 5-17
VLAN switch port table parameters 4-6
port PACE priority
10/100 port parameter 5-25
gigabit port parameters 5-18
PORT SETTINGS 1-26
port VLAN
3Com SuperStack parameters 5-37
Bay Networks System 5000 parameters 5-38
Cisco Catalyst 5000 parameters 5-37
switch port configuration parameters 5-31
switch port parameter 5-29
port VLAN parameters
configuring 5-33, 5-35
port-based VLANs 4-3
power supply
power system statistical parameters 3-16
power system statistical parameters
current power available 3-16
power supply 3-16
status 3-16
total system power 3-16
type 3-16
power system statistics
displaying 3-15
power-up/reset image
CPU redundancy configuration 7-10
PPP console
configuring 2-21
configuring a network mask 9-86
configuring an IP address 9-86
PPP console settings
baud rate 2-19
flow control 2-19
PPP console static route
configuring 9-85
PPP serial port console 2-26
regaining access to the CLI 2-24
PRE
forwarding cache (FE) parameters 18-11
Layer 3 route cache search parameters 18-9
precedence
IPX RIP filter parameters 13-4
IPX SAP filter parameters 14-5
IPX SAP network filter parameters 14-9
preference
IP static route parameters 9-25
preferences
IRDP parameters 9-79
primary controller
replacing 7-5
primary server
RADIUS configuration parameters 8-5
primary server IP address
LDAP configuration parameters 9-82
primary server port
LDAP configuration parameters 9-82
priority
address forwarding table parameters 6-11
spanning tree bridge level parameters 4-10
spanning tree bridge port information parameters 4-13
VRRP configuration parameters 9-75
priority queuing,definition 1-13
priority threshold
buffer management table parameters 20-6
probe message received
DVMRP global statistical parameters 9-59
probe messages transmitted
DVMRP global statistical parameters 9-59
process leave packets
IGMP interface parameters 9-32
producer signal
LDAP statistics 9-84
Prominent MIBs C-1
protocol
Layer 3 route cache search parameters 18-8
protocol event log
configuring 17-7, 17-10
protocol event log settings
debug 17-10
error 17-10
fault 17-10
info 17-10
trace 17-10
warning 17-10

protocol ID
IP access list parameters 9-19
proxy ARP
add IP interface parameters 9-7
IP global configuration parameters 9-9
IP interface parameters 9-3
proxy mode
LGMP server configuration parameters 16-24
prune expiration
DVMRP downstream link parameters 9-70
prune expiration time
upstream prune information 9-69
prune messages received
DVMRP global statistical parameters 9-59
prune messages transmitted
DVMRP global statistical parameters 9-59
pruning client ports, router ports, dynamic sessions
pruning client ports 16-4
purge TTL
RIP global configuration parameters 10-2

Q

query messages received
IGMP interface statistical parameters 9-54
query messages transmitted
IGMP interface statistical parameters 9-54
query request interval
IGMP interface parameters 9-32
query response interval
IGMP interface parameters 9-33
queues
managing 20-2, 20-7
service ratio 20-2

R

RADIUS
overview 8-3
RADIUS client
configuring 8-4, 8-5
RADIUS configuration parameters
Cajun-Service-Type required 8-5
enable state 8-5
group 8-5
primary server 8-5
realm 8-5
retry number 8-5
retry time 8-5
secondary server 8-5
shared secret 8-5
source IP address 8-5
UDP port 8-5
RADIUSsecondary server
shared secret 8-5
rate limit burst size
10/100 port parameter 5-25
rate limit mode
10/100 port parameter 5-25
rate limit rate
10/100 port parameter 5-25
read-only
SNMP access level 2-14
read-write
SNMP access level 2-14
read-write with security level set to admin
SNMP access level 2-15
realm
RADIUS configuration parameters 8-5
receive new LSA count
OSPF statistical parameters 11-17
receive version
RIP interface parameters 10-4
recurring
summer time hours configuration 3-8
redundant controllers
installing 7-3
redundant CPU
configuring 7-8
redundant element 7-2
configuring 7-6
related documents xxxiv
Remote Authentication Dial-In User Service (RADIUS) Client Support 1-21
remote fault detect
gigabit port parameters 5-18
remote fault detection 5-17
replacing the primary controller 7-5
report messages received
DVMRP global statistical parameters 9-59
report messages transmitted
DVMRP global statistical parameters 9-59
reporting router
DVMRP route table parameters 9-64
reporting router interface
DVMRP route table parameters 9-64
requests received
IPX SAP interface statistical parameters 14-

13
resetting the switch A-6
Resetting the Switch Using the Web Agent A-6
resource
event class parameters 17-15
retransmit interval
OSPF interface parameters 11-8
OSPF virtual link parameters 11-10
retry number
RADIUS configuration parameters 8-5
retry time
RADIUS configuration parameters 8-5
RIP
add IP interface parameters 9-7
creating trusted RIP neighbors 10-5, 10-6, 10-7
event class parameters 17-16
IP interface parameters 9-3
IPX interface 12-9
RIP 12-6
trusted neighbors 10-5, 10-6, 10-7
RIP ext type
OSPF global configuration parameters 11-3
RIP global configuration 10-1
RIP global configuration parameters
global RIP 10-2
purge TTL 10-2
triggered updates 10-2
update pkt delay 10-2
update timer 10-2
RIP interface parameters
auth key 10-5
auth type 10-5
default metric 10-4
default route 10-4
interface 10-3
mode 10-4
network address 10-3
receive version 10-4
split horizon 10-4
version 10-4
RIP interfaces
configuring 10-3
RIP packet tracing
enabling 17-7, 17-10
RIP queries
IP routing table statistical parameters 9-49
RIP route changes
IP routing table statistical parameters 9-49
RIP routes
IP global configuration parameters 9-10
RIP statistical parameters
bad packets received 10-8
bad routes received 10-8
interface 10-8
IP address 10-8
non-trigger updates sent 10-8
state 10-8
triggered updates sent 10-8
updates received 10-8
RIP statistics
interpreting 10-7, 10-8
RMON
configuring a mirror port 19-8, 19-12
RMON mirror port configuration parameters
mirror port 19-10
piggyback port 19-11
port 19-10
sampler type 19-12
RMON statistics
viewing 19-1, 19-7
robustness variable
IGMP interface parameters 9-33
IGMP interface statistical parameters 9-54
LGMP server configuration parameters 16-25
route add failures
IPX routing table statistic 12-22
route metric
DVMRP route table parameters 9-64
route preference by protocol
IP global configuration parameters 9-9
router cost to source network
DVMRP upstream routers 9-65
router ID
LSA detail 11-27
OSPF global configuration parameters 11-3
OSPF link state database parameter 11-26
OSPF link state database search parameters 11-24
OSPF neighbors parameters 11-21
OSPF statistical parameters 11-17
OSPF virtual link parameters 11-10
router is SNMP manageable
DVMRP downstream dependent router 9-

67
router network address
DVMRP downstream dependent router 9-67
DVMRP upstream routers 9-65
router port display parameters
application 16-9
port 16-9
VLAN 16-9
Router ports 16-2
router ports 16-8
router ports removed
IGMP snooping 16-21
router pruning timer
router pruning timer 16-7
router received probe from this router
DVMRP downstream dependent router 9-67
router report time
LGMP server configuration parameters 16-25
router supports generation ID function
DVMRP downstream dependent router 9-67
router supports prune function
DVMRP downstream dependent router 9-67
routing
hardware requirements 9-11, 12-4
Layer 2 overview 1-29
Layer 3 (learned) overview 1-29
Layer 3 (not learned) overview 1-29
Layer 3 overview 1-29
Layer 3 switching 9-11
routing configuration
minimum requirements 9-11
Routing with Layer 2 and Layer 3 Modules 1-28
RTMP RDR Rx
AppleTalk global statistics 15-25
RTMP RDR Tx
AppleTalk global statistics 15-25
RTMP Rq Rx
AppleTalk global statistics 15-25
RTMP Rq Tx
AppleTalk global statistics 15-25
RTMP Rsp Rx
AppleTalk global statistics 15-25
RTMP Rsp Tx
AppleTalk global statistics 15-25
rule number
Layer 3 route cache search parameters 18-9
running configuration
viewing 2-27
running.txt 2-27
RX frame count (T2)
frame forwarding statistical parameters 18-6
RX LED
behavior 17-1

S

sample
Ethernet interface statistical parameters 19-4
sampler type
port mirroring information parameters 19-9
RMON mirror port configuration parameters 19-12
SAP
SAP 12-6, 12-10
save running configuration to startup configuration
configuration file management 2-30
saving your current configuration A-2
search base
LDAP configuration parameters 9-83
searching the routing cache 18-7
Searching the Routing Cache for an Entry 18-7, 18-9, 18-12
secondary server
RADIUS configuration parameters 8-5
secondary server IP address
LDAP configuration parameters 9-82
secondary server port
LDAP configuration parameters 9-83
security level
configuring SNMP communities 2-16
security levels
SNMP 2-16
seed
AppleTalk interface statistics 15-26
Select 9-79
Selecting the Image for Reboot Using the Web Agent A-4, A-5
sequence

LSA detail 11-27
OSPF link state database parameter 11-26
server ID priority
LGMP server configuration parameters 16-25
service name
IPX service table search parameter 12-23
IPX static service parameter 12-15
service port status
event class parameters 17-15
service ratio (queues) 1-28, 20-2
service type
IPX service table search parameter 12-23
session ID
multicast session parameters 16-12
session pruning timer
session pruning timer 16-7
session search
intelligent multicast 16-10, 16-13
sessions destroyed
IGMP snooping 16-21
set recurring
summer time hours 3-6, 3-9
setting all ports in a module 5-26
setting summer time hours 3-4
one time 3-10, 3-12
setting switch ports on all modules 5-41
setting the system clock 3-3
setting up user accounts 2-11
severity
event and shutdown log entries 17-12
shared secret
RADIUS configuration parameters 8-5
RADIUS secondary server 8-5
Short PDU in error
AppleTalk global statistics 15-24
shutdown log
definition 17-15
shutdown log (switch event)
definition 17-7
shutdown temperature
temperature threshold parameter 17-4
size
address table instance hash table parameter 6-7
SNMP
communities 2-13
security levels 2-16
SNMP access level
none 2-15
read-only 2-14
read-write 2-14
read-write with security level set to admin 2-15
SNMP Administration 2-13, 2-17, 2-21
SNMP communities, configuring 2-13, 2-16
access level 2-14
IP address 2-14
security level 2-16
trap receiver 2-16
SNMP security level
admin 2-16
normal 2-16
snmp version supported 2-13
SNTP
enabling 3-3, 3-4
socket
IPX service table parameter 12-24
IPX static service parameter 12-15
source
IP routing table search parameters 9-47
IPX route table parameter 12-21
IPX routing table search parameters 12-20
IPX service table parameter 12-25
IPX service table search parameter 12-23
source address
Layer 3 route cache search parameters 18-8
source address mask
DVMRP multicast forwarding cache parameters 9-68
IGMP local multicast forwarding cache parameters 9-57
source filename
configuration file management 2-31
source IP address
RADIUS configuration parameters 8-5
source network
DVMRP route table parameters 9-64
IPX datagram fields 12-3
source network mask
DVMRP route table parameters 9-64
source node
IPX datagram fields 12-3
source port
Layer 3 route cache search parameters 18-8
port mirroring information parameters 19-

9
source port number
DVMRP upstream source parameters 9-70
source socket
IPX datagram fields 12-3
source subnetwork
DVMRP downstream link parameters 9-69
DVMRP multicast forwarding cache parameters 9-68
IGMP local multicast forwarding cache parameters 9-57
upstream prune information 9-68
spanning tree 4-9
non-VLAN switch port parameters 5-36
path cost 4-14
using for setup and monitoring 4-8
spanning tree bridge level parameters
bridge forward delay 4-10
bridge hello time 4-10
bridge max age 4-10
forward delay 4-10
hello time 4-10
max age 4-10
mode 4-10
priority 4-10
spanning tree bridge port
blocking state 4-12
disabled 4-12
down state 4-12
forwarding state 4-12
learning state 4-12
listening state 4-12
spanning tree bridge port information
top change detection 4-14
spanning tree bridge port information parameters
enable 4-13
path cost 4-14
priority 4-13
spanning tree bridge port parameters
bridge port 4-12
designated bridge 4-12
designated cost 4-12
designated port 4-12
designated root 4-12
forward transitions 4-12
name 4-12
port 4-12
state 4-12
spanning tree bridge ports
configuring 4-11
spanning tree mode
switch port configuration parameters 5-32
spanning tree mode for a port 4-15
Spanning Tree Protocol 1-8
speed mode
10/100 port parameter 5-24
SPF hold time
OSPF global configuration parameters 11-3
SPF runs
OSPF statistical parameters 11-18
SPF suspend
OSPF global configuration parameters 11-3
split horizon
RIP interface parameters 10-4
SSM 1-16
stale drops
buffer management table parameters 20-6
STAP mode
switch port parameter 5-29
start
event class parameters 17-15
one-time summer time hours configuration 3-11
summer time hours configuration 3-8
start network
IPX RIP filter parameters 13-4
startup config
CPU redundancy configuration 7-10
startup configuration
viewing 2-27
startup.txt 2-27
state
AppleTalk interface statistics 15-26
AppleTalk route table statistics 15-28
DVMRP interface statistical parameters 9-60
IGMP interface statistical parameters 9-54
IP interface parameters 9-3
IPX interface 12-9
IPX SAP interface statistical parameters 14-13
LGMP server display per VLAN parameters 16-28
OSPF link parameters 11-19
OSPF neighbors parameters 11-21

RIP statistical parameters 10-8
spanning tree bridge port parameters 4-12
VRRP statistical parameters 9-77
static
Virtual LAN binding options 5-35
static address configuration
adding entries to the address forwarding table 6-12
static client port
creating 16-18, 16-19
static client ports
deleting 16-19
static multicast session parameters 16-17
static ext type
OSPF global configuration parameters 11-3
static low ext type
OSPF global configuration parameters 11-3
static multicast session configuration parameters
IP address 16-16
MAC address 16-16
VLAN 16-16
static multicast session parameters
IP address 16-17
MAC address 16-17
static client ports 16-17
VLAN 16-17
static multicast session, creating
creating a static multicast session 16-15, 16-16
static multicast sessions, configuring
configuring static multicast sessions 16-17, 16-18
static route
PPP console 9-85
static route, AppleTalk 15-10
static routes
IPX
deleting 12-12, 12-13
status
address forwarding table parameters 6-12
CPU redundancy configuration 7-10
power system statistical parameters 3-16
stop bits
console serial port settings 2-19
stub metric
OSPF area parameters 11-5
summer time hours
one-time setting 3-10, 3-12
set recurring 3-6, 3-9
setting 3-4
summer time hours configuration
day 3-9
end 3-8
hour 3-9
minutes 3-9
month 3-9
recurring 3-8
start 3-8
week 3-8
super age time
definition 6-1
supervisor module configuration
CLI 2-3
supported browsers 2-8
switch
resetting A-6
switch configuration
managing 2-28
switch description 1-1
switch design supported features 1-19
switch design,definition
MAC Address 1-19
optional per-VLAN spanning tree 1-19
segmented address tables 1-19
switch fabric
event class parameters 17-16
switch features
crossbar switch fabric,overview 1-5, 1-7
switch port
configuring 5-30
switch port configuration
enabling fast start mode 5-39, 5-41
switch port configuration parameters
3Com mapping table 5-32
allow learning 5-32
automatic VLAN creation 5-32
fast start 5-32
frame tags 5-31
hunt group 5-32
known mode 5-32
mirror port 5-32
port VLAN 5-31
spanning tree mode 5-32
trunk mode 5-31
VLAN binding 5-31

VTP snooping 5-32
switch port parameters
hunt group 5-29
links 5-29
MAC address 5-29
name 5-29
port 5-29
port VLAN 5-29
STAP mode 5-29
trunk mode 5-29
viewing 5-28
VLAN classification 5-29
switch ports, single command 5-41
Synchronizing the Primary and Redundant CPUs 7-9
system
event class parameters 17-15
system information
editing 3-2
system information, changing
contact 3-2
location 3-2
system reset
performing 3-18

T

tag
LSA detail 11-28
TblInst
address forwarding table parameters 6-11
TCP established
IP access list parameters 9-20
TCP/UDP destination port
IP access list parameters 9-20
TCP/UDP source port
IP access list parameters 9-19
Technical Support
contacting xxx
technical support
contacting xxx
temperature status
event class parameters 17-15
viewing 17-2, 17-3, 17-5
temperature system
configuring 3-14, 3-15
temperature threshold parameters
low shutdown temperature 17-4
lower warning temperature 17-4
shutdown temperature 17-4
upper warning temperature 17-4
temperature thresholds 17-4
terminal setup 2-2
TFTP server
copying 2-31
TFTP server IP address
configuration file management 2-31
TFTP transfer status
viewing 2-33
this router is group membership querier
IGMP interface statistical parameters 9-54
Throughput 1-5, 1-7
ticks
IPX RIP filter parameters 13-5
IPX route table parameter 12-21
IPX static route 12-12
time of state change
VRRP statistical parameters 9-77
time stamp
event and shutdown log entries 17-12
times this VR became master
VRRP statistical parameters 9-77
too long
AppleTalk global statistics 15-24
too short
AppleTalk global statistics 15-24
top change detection
spanning tree bridge port information 4-14
T-option
OSPF neighbors parameters 11-22
TOS
LSA detail 11-27
TOS 0 metric
LSA detail 11-27
TOS count
LSA detail 11-27
total bucket utilization 6-7
total entries
forwarding cache (FE) parameters 18-11
total number of entries
address table instance parameters 6-6
total routes added
IP routing table statistical parameters 9-49
total routes deleted
IP routing table statistical parameters 9-49
total system power
power system statistical parameters 3-16
trace
protocol event log settings 17-10

traffic flooding 19-8
traffic mirror port 19-10
transit delay
  OSPF interface parameters 11-7
  OSPF virtual link parameters 11-10
translate 7 into 5
  OSPF area parameters 11-5
transport control
  IPX datagram fields 12-3
trap
  event table actions 17-17
trap receiver
  configuring SNMP communities 2-16
triggered updates
  IPX SAP interface parameters 14-3
  RIP global configuration parameters 10-2
triggered updates sent
  IPX SAP interface statistical parameters 14-13
  RIP statistical parameters 10-8
trunk mode
  3Com SuperStack parameters 5-37
  Bay Networks System 5000 parameters 5-38
  Cisco Catalyst 5000, parameters 5-37
  switch port configuration parameters 5-31
  switch port parameter 5-29
TTL
  AppleTalk ARP cache table statistics 15-31
  IPX route table parameter 12-21
  IPX service table parameter 12-25
  purge 10-2
TTL expired
  AppleTalk global statistics 15-24
TTY console settings
  baud rate 2-19
  data bits 2-19
  flow control 2-19
  parity 2-19
  stop bits 2-19
tunnel endpoint address
  DVMRP interface parameters 9-38
TX LED
  behavior 17-1
type
  AppleTalk ARP cache table statistics 15-31
  AppleTalk NBP filter parameters 15-15
  AppleTalk NBP table parameters 15-34
  AppleTalk static route 15-11
  AppleTalk zone filter parameters 15-19
  DVMRP interface statistical parameters 9-61
  event and shutdown log entries 17-12
  forwarding cache (FE) parameters 18-11
  IPX SAP filter parameters 14-6
  IPX SAP network filter parameters 14-9
  IPX service table parameter 12-24
  IPX static service parameter 12-15
  LSA detail 11-26
  multicast session parameters 16-12
  OSPF link parameters 11-19
  OSPF link state database parameter 11-25
  OSPF link state database search parameters 11-24
  power system statistical parameters 3-16
type (network)
  LSA detail 11-27
type 20 packet propagation
  IPX interface 12-10
type 3 ASE filter
  OSPF area parameters 11-5

U

UDP in datagrams
  IP routing global statistics 9-44
UDP in errors
  IP routing global statistics 9-44
UDP out datagrams
  IP routing global statistics 9-44
UDP port
  RADIUS configuration parameters 8-5
undersize packets
  Ethernet interface statistical parameters 19-6
unknown messages codes encountered
  DVMRP global statistical parameters 9-59
unknown messages received
  IGMP global statistic parameters 9-52
  IGMP interface statistical parameters 9-55
unrecognized packets received
  DVMRP interface statistical parameters 9-61
UPD in no ports
  IP routing global statistics 9-44
update pkt delay
  RIP global configuration parameters 10-2
update timer
  RIP global configuration parameters 10-2

update timestamp
VTP snooping parameters 4-33
updater identity
VTP snooping parameters 4-33
updater time stamp
VLAN exchange parameters 4-33
updates received
IPX SAP interface statistical parameters 14-13
RIP statistical parameters 10-8
upgrading from a previous version of software A-1
upper warning temperature
temperature threshold parameter 17-4
upstream interface
DVMRP multicast forwarding cache parameters 9-68
IGMP local multicast forwarding cache parameters 9-57
upstream interface is pruned
DVMRP multicast forwarding cache parameters 9-68
upstream neighbor router address
DVMRP multicast forwarding cache parameters 9-68
upstream prune information
destination group address 9-68
DVMRP upstream interface 9-69
interface is pruned 9-69
interface type 9-69
prune expiration time 9-69
source subnetwork 9-68
upstream router
DVMRP route table parameters 9-65
upstream source
IGMP local multicast forwarding cache parameters 9-57
upstream sources 9-70
DVMRP multicast forwarding cache parameters 9-68
use default route
use default route 12-6
use default route for proxy ARP
IP global configuration parameters 9-9
use interpacket gap
IPX SAP interface parameters 14-2
use max packet size
IPX SAP interface parameters 14-2
user accounts
setting up 2-11
user logins
default 2-11
user port status
event class parameters 17-15
using dial-up networking
using dial-up networking 2-26
utilization
Ethernet interface statistical parameters 19-4

V

valid
address forwarding table parameters 6-11
version
RIP interface parameters 10-4
view the active alarm table 17-6
viewing AppleTalk global statistics 15-23, 15-25
viewing AppleTalk route table statistics 15-29
viewing AppleTalk statistics 15-22
viewing AppleTalk zone table statistics 15-33
viewing DVMRP downstream routers 9-66
viewing DVMRP neighbor routers 9-61
viewing DVMRP upstream routers 9-65
viewing Ethernet statistics 19-1, 19-7
viewing event and shutdown logs 17-11, 17-13
viewing event statistics 17-13, 17-14, 17-16
viewing IGMP interface statistics 9-52, 9-55
viewing RMON statistics 19-1, 19-7
viewing switch port parameters 5-28
Viewing Switch Port Parameters Using the CLI 5-29
viewing the AppleTalk ARP cache table 15-30, 15-31
viewing the AppleTalk NBP table 15-34
Viewing the AppleTalk Route Table 15-27
viewing the AppleTalk route table 15-27
viewing the AppleTalk zone table 15-32
viewing the downloaded image A-4
viewing the running configuration 2-27
viewing the script execution log file
script execution log file viewing 2-28
viewing the startup configuration 2-27
Viewing the Status of a TFTP Transfer 2-33
viewing the TFTP transfer status 2-33

viewing VRRP statistics 9-76, 9-78
Virtual 1-19
Virtual Bridging Functions 1-19
Virtual LAN binding options
  bind to all 5-35
  bind to received 5-35
  static 5-35
Virtual LANs
  binding options 5-35
  flood pruning overview 1-19
  trunk mode, configuring 5-33
virtual LANs
  creating a VLAN 4-4
  parameters 4-4
Virtual LANs, configuring
  automatic VLAN creation 5-34
  trunk mode 5-33
  VLAN binding 5-34
virtual router
  VRRP 9-74, 9-76
virtual routers
  enabling VRRP 9-73
VLAN
  add IP interface parameters 9-6
  AppleTalk interface parameters 15-5
  ARP cache search parameters 9-50
  configuring all ports 4-5
  creating 4-4
  egress rules 4-3
  filtering 6-9
  forwarding rules 4-2
  IP interface parameters 9-3
  IPX interface 12-9
  Layer 3 route cache search parameters 18-8
  LGMP client display per VLAN parameters 16-33
  LGMP server display per VLAN parameters 16-28
  multicast session parameters 16-12
  operation 4-1
  router port display parameters 16-9
  search 6-9
  static multicast session configuration parameters 16-16
  static multicast session parameters 16-17
VLAN association
  address table instance parameters 6-6
VLAN binding
  Cisco Catalyst 5000 parameters 5-37
  switch port configuration parameters 5-31
VLAN binding, configuring
  Virtual LANs 5-34
VLAN bindings
  3Com SuperStack parameters 5-38
  Bay Networks System 5000 parameters 5-38
VLAN classification
  switch port parameter 5-29
VLAN configuration parameters
  auto increment HT size 4-5
  initial hash table size 4-5
VLAN considerations 4-3
VLAN exchange parameters
  updater timestamp 4-33
VLAN operation
  ingress rules 4-2
VLAN Operational Rules 5-7
VLAN spanning tree bridge level parameters
  bridge forward delay 4-10
  bridge hello time 4-10
  bridge max age 4-10
  forward delay 4-10
  hello time 4-10
  max age 4-10
  mode 4-10
  priority 4-10
VLAN switch port table parameters
  binding type 4-6
  frame format 4-6
  port 4-6
  port name 4-6
VLAN trunking,definition 1-13
VR ID
  VRRP configuration parameters 9-75
  VRRP statistical parameters 9-77
VRRP
  add IP interface parameters 9-7
  enabling 9-71, 9-73
  IP global configuration parameters 9-9
  IP interface parameters 9-4
VRRP configuration overview 9-71
VRRP configuration parameters
  addr owner override 9-76
  advertisement timer 9-75
  auth key 9-76
  interface 9-75
  IP address 9-75

priority 9-75
VR ID 9-75
VRRP overview
configuring 9-71
VRRP router
creating 9-74
VRRP statistical parameters
advertisements received 9-77
advertisements sent 9-77
bad advertisements received 9-77
interface 9-77
IP address 9-77
state 9-77
time of state change 9-77
times this VR became master 9-77
VR ID 9-77
VRRP statistics
viewing 9-76, 9-78
VRRP virtual router
creating 9-74, 9-76
VTP snooping
Cisco Catalyst 5000 parameters 5-37
VTp snooping
switch port configuration parameters 5-32
VTP snooping parameters
configuration revision number 4-33
domain name 4-33
update timestamp 4-33
updater identity 4-33
VTP snooping state 4-33
VTP snooping state
VTP snooping parameters 4-33

W

warning
protocol event log settings 17-10
Web Agent
logging into 2-8
setting up user accounts 2-11
week
one-time summer time hours configuration 3-11
summer time hours configuration 3-8

X

Xon/Xoff
flow control 2-19

Z

Zip Ext Reply Rx
AppleTalk global statistics 15-25
Zip Ext Reply Tx
AppleTalk global statistics 15-25
Zip GNI Rq Rx
AppleTalk global statistics 15-25
Zip GNI Rq Tx
AppleTalk global statistics 15-25
Zip GNI Rsp Rx
AppleTalk global statistics 15-25
Zip GNI Rsp Tx
AppleTalk global statistics 15-25
Zip Query Rx
AppleTalk global statistics 15-25
Zip Query Tx
AppleTalk global statistics 15-25
Zip Reply Rx
AppleTalk global statistics 15-25
Zip Reply Tx
AppleTalk global statistics 15-25
zone
AppleTalk interface parameters 15-6
AppleTalk NBP table parameters 15-34
AppleTalk static route 15-11
zone filter
adding interfaces 15-21, 15-22
creating 15-18
deleting interfaces 15-21, 15-22
editing 15-20
zones
AppleTalk route table statistics 15-28